Universidade Federal do Rio de Janeiro

Raphael Carlos Santos Machado

SISTEMAS DINÂMICOS E CRIPTOSSISTEMAS

(Volume Único)

Rio de Janeiro
2006

Raphael Carlos Santos Machado

SISTEMAS DINÂMICOS E CRIPTOSSISTEMAS

(Volume Único)

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática Aplicada, do Instituto de Matemática, Centro de Ciências Matemáticas e da Natureza, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Ciências (Matemática Aplicada).

Orientador: Ricardo Martins da Silva Rosa

Rio de Janeiro
2006

M149S Machado, Raphael Carlos Santos
Sistemas Dinâmicos e Criptossistemas / Raphael Carlos Santos Machado. – Rio de Janeiro : UFRJ/IM, 2006.
122f.; 29cm.

Dissertação (mestrado). – Programa de Pós-Graduação em Matemárica Aplicada, 2006.
Orientador: Ricardo Martins da Silva Rosa

1. Sistemas Dinâmicos – Tese. I.Rosa, Ricardo Martins da Silva (orient.). II. Universidade Federal do Rio de Janeiro. Instituto de Matemática. III. Título.

CDD: 515.352

SISTEMAS DINÂMICOS E CRIPTOSSISTEMAS

Autor: Raphael Carlos Santos Machado

Orientador: Ricardo Martins da Silva Rosa

Dissertação de Mestrado submetida ao Programa de Pós-Graduação em Matemática Aplicada, do Instituto de Matemática, Centro de Ciências Matemáticas e da Natureza, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Ciências (Matemática Aplicada).

Aprovada por:

_____
Presidente, Professor Ricardo Martins da Silva Rosa, UFRJ

_____
Professora Isabel Lugão Rios, UFF

_____
Professor Felipe Acker, UFRJ

_____
Professor Marco Aurélio Palumbo Cabral, UFRJ

Rio de Janeiro

Julho 2006

RESUMO

MACHADO, Raphael Carlos Santos Machado. **Sistemas Dinâmicos e Criptossistemas**. Rio de Janeiro, 2006. Dissertação (Mestrado em Matemática Aplicada) – Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006

Estudo das conexões entre Sistemas Dinâmicos e Criptografia. Levantamento das principais aplicações de Sistemas Dinâmicos, e particularmente de sistemas caóticos, à elaboração de criptossistemas teóricos e práticos. Identificação e classificação de ataques a criptossistemas caóticos. Investigação das relações entre os conceitos teóricos das duas disciplinas e de possíveis aplicações da Teoria Ergódica ao estudo de criptossistemas teóricos contínuos.

ABSTRACT

MACHADO, Raphael Carlos Santos Machado. **Sistemas Dinâmicos e Criptossistemas**. Rio de Janeiro, 2006. Dissertação (Mestrado em Matemática Aplicada) – Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006

Study of the conexions between Dynamical Systems and Cryptossystems. Survey of the mainn applications of Dynamical Systems, and particularly chaotic systems, to the construction os theoretical and practical cryptossystems. Identification and classification of chaotic cryptossystems attacks. Investigation of relations between the theoretical concepts of both disciplines, and of possible applications of Ergodic Theory to the study of continuous theoretical criptossystems.

Śumario

´

Introdução

Histórico dos Criptossistemas Caóticos

Há muito tempo pesquisadores têm apontado relações entre caos e criptografia: as conexões entre as duas disciplinas têm sido mencionadas desde antes do surgimento da própria denominação de "caóticos" para certos sistemas com propriedades complexas. Em seu clássico trabalho [3], Shannon menciona que transformações interessantes à comunicação segura, poderiam ser construídas a partir das operações básicas "esticar" e "dobrar". Características de sistemas caóticos como sensibilidade às condições iniciais, ergodicidade e mistura ("mixing") têm sido relacionadas com as propriedades de confusão e difusão de transformações criptográficas. É natural, assim, buscar aplicações na criptografia para as técnicas de sistemas dinâmicos e, ao mesmo tempo, estudar sistemas caóticos através de conceitos de criptografia. (Ao longo do texto, usaremos o termo "criptografia caótica" para nos referirmos a criptossistemas que, de alguma forma, utilizam sistemas caóticos.)

Os primeiros artigos sobre "criptografia caótica" parecem ter sido [9], de 1985, e [10], de 1987, onde se descrevem criptossistemas baseados em autômatos celulares, mas que não tiveram muita repercussão entre os pesquisadores. Em 1989, Matthew [11] publica artigo em que descreve um cifrador de "streams" (onde cada caractere é codificado individualmente) baseado em um mapa logístico generalizado,

e que causa um primeiro "boom" de trabalhos na área de criptografia caótica. Em 1990, Pecora et al. [14] iniciam uma série de estudos em que demonstram a possibilidade de sincronização de sistemas caóticos e aplicam o conceito à comunicação de sinais analógicos. Este último trabalho foi outro grande responsável pela atenção da comunidade científica às aplicações de caos à comunicação e à segurança de dados.

O boom inicial durou cerca de 4 anos, ao longo dos quais uma formidável quantidade de trabalhos foi publicada. No entanto, a maioria dos criptossistemas apresentado nesses trabalhos acabou mostrado-se fraca e o interesse por criptografia caótica reduziu-se bastante (assim como a publicação de artigos) nos anos de 1993 a 1996. A partir de 1997 observou-se uma retomada do interesse por criptossistemas caóticos, principalmente com a divulgação de uma série de novos criptossistemas ([**?**, 32, 27, 28, 29], por exemplo). Observou-se, também, a retomada do interesse pelas conexões matemáticas entre caos e criptografia: embora o foco da maioria dos trabalhos ainda fosse o de mostrar aplicações de sistemas caóticos à criptografia, observou-se a preocupação e pelo menos sugerir possíveis conexões entre as disciplinas. Apesar de se verificar um consenso entre os pesquisadores a respeito da importância do desenvolvimento de uma teoria matemática que explicasse essas conexões, não foi possível localizar nenhum artigo em que se buscasse explicitamente esse objetivo.

Contribuições desta dissertação

O interesse do autor nos cifradores caóticos estudados nesta dissertação foi inicialmente motivado ao tomar contato com artigos sobre a sincronização de caos e suas possíveis aplicações à comunicação de dados. As referências destes artigos acabaram levando à criptografia caótica digital, campo cujas aplicações pareceram bem mais práticas e exeqüíveis, mas cujos trabalhos muitas vezes careciam de maior rigor e

análises mais detalhadas de segurança. As contribuições desta dissertação são relacionadas com três aspectos:

1) Relações entre sistemas dinâmicos e criptografia. Investigamos possíveis definições matemáticas para as propriedades de difusão e confusão, consideradas as mais importantes propriedades de bons criptossistemas, e sempre relacionadas com características de sistemas caóticos, mas nunca definidas de forma precisa. Apesar de as definições tradicionais desses conceitos serem pouco precisas e dificultarem o estabelecimento de uma conexão com sistemas caóticos, acreditamos ter alcançado um novo entendimento para estes conceitos que permite esta conexão.

2) Classificação e análise dos principais criptossistemas digitais baseados em caos propostos nas últimas duas décadas. O estudo desses trabalhos permitiu a identificação das principais falhas desses criptossistemas, e a elaboração de uma série de recomendações para a elaboração de criptossistemas seguros.

3) Estudo da sincronização do caos e suas possibilidades de aplicação à comunicação analógica segura. Analisamos os principais esquemas propostos desde os primeiros trabalhos na área e identificamos classes básicas de ataques a estes esquemas, descritos no capítulo sobre sincronização.

Além dessas contribuições, ao longo dos estudos para a elaboração desta dissertação, foi possível recuperar uma enorme quantidade de trabalhos sobre criptografia caótica desde a década de 80, de forma que tornou-se possível levantar um breve histórico das atividades e produção científica na área. Particularmente identificou-se dois booms, o primeiro, no início da década de 90 e o segundo, a partir de 1997 (e que parece durar até o presente).

Por se tratar de um campo multidisciplinar, localizaram-se trabalhos sobre criptografia caótica em periódicos relacionados à Fisica, à Matemática e à Engenharia. Apesar da grande quantidade de artigos, poucos apresentaram um tratamento matemático realmente rigoroso dos problemas e questões abordadas. A inexistência de um ferramental matemático estabelecido para o estudo das propriedades caóticas de criptossistemas tornou difícil o estudo destes sistemas, de forma que o caminho seguido nesta dissertação para a investigação dessas propriedades foi, muitas vezes, o conceitual, e até intuitivo, em detrimento de uma abordagem matemática estrita que, neste estágio, poderia tornar ainda mais nebulosas as idéias apresentadas. Acreditamos que esta dissertação é um primeiro passo para o objetivo de desenvolver métodos matemáticos mais rigorosos para o estudo da Criptografia. O caminho para o desenvolvimento de tais métodos parece ser a união das técnicas e conceitos de Análise Combinatória inspiradas pelas idéias de Sistemas Dinâmicos. O autor pretende prosseguir com suas investigações sobre a matemática dos criptossistemas em seus estudos de Doutorado.

Chapter 1

Aplicações de Caos à Criptografia Digital

Este capítulo serve de motivação. Fazemos uma introdução à criptografia clássica e um levantamento de estudos em criptografia caótica. Analisamos as diversas abordagens utilizadas em criptografia caótica, identificando suas principais características. Ao final do capítulo, compilamos um roteiro com os principais requisitos para a construção de bons criptossistemas caóticos.

1.1 Terminologia e Conceitos de Criptografia

1.1.1 Breve Histórico da Criptografia

As técnicas de criptografia são, de certa forma, conhecidas desde a antigüidade. Os primeiros registros de uso de técnicas criptográficas datam do século XIX A.C., quando um escriba egípcio utilizou uma variação dos hieróglifos-padrão da época para comunicar-se. O Kama-sutra, aproximadamente do ano 400 A.C., recomenda o estudo pelas mulheres da "arte da escrita secreta". Na Bíblia, o livro de Jeremias usa um código extremamente simples do alfabeto hebreu para a história de Babel: a primeira letra do alfabeto hebreu (Aleph) é trocada pela última (Taw), a segunda letra (Beth)

e trocada pela penúltima (Shin) e assim sucessivamente. Destas quatro letras deriva o nome da cifra: Aleph Taw Beth SHin - ATBASH. A cifra ATBASH data de cerca de 600 A.C.. Júlio César (100-44 A.C.) utilizava uma cifra de substituição simples em comunicações com membros do governo.

A Idade Média apresenta alguns registros de avanços em criptografia. Al-Kindi, no século IX D.C., escreve um tratado sobre a decifração de mensagens criptográficas que ainda está conservado e, hoje, é considerado o livro mais antigo de criptologia. No livro, Al-Kindi introduz as análises de freqüência para a investigação e quebra de criptogramas. No século XII D.C., Al-Khalil escreve, para o imperador bizantino, um livro de criptografia, mas que infelizmente se perdeu. Al-Khalil decifrou um criptograma bizantino antigo ao supor, corretamente, que o início do texto seria a expressão "em nome de Deus" (algo comum na época) criando a técnica da "palavra provável". A Idade Moderna apresenta avanços significativos em Criptografia, com as importantes contribuições de nomes como Girolamo Cardano, Blaise de Vigenère e Sir Francis Bacon, entre outros.

Em torno de 1795, Thomas Jefferson, possivelmente com a ajuda do Dr. Robert Patterson, um matemático da Universidade da Pensilvânia, inventa um cilindro cifrador (ou cifra de roda). Apesar da engenhosidade deste dispositivo composto por 26 discos, ele nunca chegou a ser utilizado. O cilindro de Jefferson permite realizar com rapidez e segurança uma substituição polialfabética. Os cilindros cifrantes são, por assim dizer, uma invenção do século XIX. Foram re-inventados por diversas vezes e utilizados pelos militares no século XX, até a Segunda Guerra Mundial. Em 1799 descobre-se a Pedra da Roseta, com a qual foi possível decifrar hieroglifos egípcios. As mensagens da pedra, que pode ser considerada um "dicionário" em três línguas, foram

decifradas somente em 1822 por Champollion, após uma tentativa frustrada feita por Thomas Young em 1814. A história é altamente interessante porque envolve conhecimento de línguas, um grande poder investigativo e uma boa dose de intuição. Charles Babbage, matemático inglês e hoje chamado de "o pai do computador", quebra a cifra de Vigenère e projeta as primeiras máquinas de cáculo sofisticadas, precursoras do computador: a "Máquina das Diferenças" e a "Máquina Analítica".

A história da criptografia desde o início do século XX até os dias atuais é repleta de histórias. Capítulos interessantíssimos aconteceram no combate a contrabandistas de bebidas durante a lei seca (os quais utilizavam códigos secretos em suas comunicações) e também nas comunicações durante a Segunda Guerra Mundial. No campo científico, destacamos o trabalho de Shannon, no final da década de 40, que definiu as bases matemáticas das teorias da Informação e da Criptografia e o trabalho de Whitfield Diffie e Martin Hellman, que introduzem, em seu livro New Directions in Cryptography (1976), a idéia de uma criptografia de chave pública. Também merecem menção, por sua importância, os trabalhos de Feistel (década de 60, desenvolve a cifra Lucifer, que alguns anos depois serviria de base para o DES e outros cifradores, criando uma família conhecida como "cifras Feistel"), de Ronald L. Rivest, Adi Shamir e Leonard M. Adleman (desenvolvem o RSA em 1977), e Miller (1986, criptografia de curvas elípticas). A partir do final da década de 80, inicia-se o desenvolvimento de uma série de trabalhos voltados para a aplicação de sistemas dinâmicos caóticos ao desenvolvimento de criptossistemas.

1.1.2 Criptossistema

Domínio e Codomínio de Encriptação

Neste texto, A irá denotar um conjunto finito que é o "alfabeto de definição", onde se encontram os "símbolos" usados na mensagem a ser encriptada. Os dois principais alfabetos nesta dissertação são o alfabeto latino ({A,B,C,...,Z}) e o alfabeto binário ({0,1}).

P denotará o espaço das "mensagens-planas", que são seqüências finitas de símbolos de um alfabeto de definição. C denotará o espaço das "mensagens-cifradas" e também consiste de seqüências de símbolos de um alfabeto de definição A', que pode ser diferente do alfabeto de definição A de P.

Transformações de Encriptação e Decriptação

K denota o conjunto chamado "espaço das chaves"; um elemento de K é chamado de "chave". Cada elemento $k \in K$ determina unicamente uma transformação injetiva de P em C, denotado por e_k, chamada transformação ou função de encriptação. Para cada $k \in K$, d_k denota uma transformação C_k em P, definida no subconjunto $C_k = e_k(P)$ de C. A transformação $d_k : C_k \rightarrow P$ é chamada de função ou transformação de decriptação.

Nesta dissertação estaremos interessados principalmente em criptossistemas de bloco, onde os espaços das mensagens-planas e das mensagens-cifradas têm a mesma cardinalidade. Neste caso, como as cardinalidades de P e de C são iguais, trataremos apenas de funções bijetivas de encriptação/decriptação.

Modelo Geral de um Criptossistema

Os conceitos gerais relacionados com criptografia e criptanálise podem ser descritos de uma maneira formal com o uso da seguinte notação matemática. Um criptossistema é uma quíntupla $(P, C, K, E = \{e_k : k \in K\}, D = \{d_k : k \in K\})$, onde as seguintes condições são satisfeitas:

1. P é o conjunto (finito) das mensagens-planas.

2. C é o conjunto (finito) das mensagens-cifradas.

3. K é o espaço (finito) das chaves.

4. Para cada $k \in K$ existe uma regra de encriptação $e_k \in E$ e uma regra de decriptação $d_k \in D$. Cada $e_k : P \to C$ e $d_k : C_k \to P$ são funções tais que $d_k(e_k(p)) = p$ para toda mensagem-plana $p \in P$. E e D representam os conjuntos de todas as regras de encriptação e decriptação, respectivamente.

Ao longo da dissertação, usaremos notações diversas para representar um criptossistema, de acordo com o contexto. Quando estivermos trabalhando com criptografia de bloco de chave simétrica (que será nosso foco na maior parte da dissertação) cada função de decriptação é facilmente deduzível a partir da função de encriptação (e vice-versa). Neste caso, denotaremos o criptossistema pela tripla $(M, K, \{T_k\})$. Nessa notação, M é o espaço das mensagens, e tanto as mensagens-planas quanto as mensagens-cifradas estão em M. $\{T_k\}$ é a família das funções de encriptação. A função de decriptação correspondente a T_k é T_k^{-1}. Outras formas de representação de um criptossistemas serão descritas ao longo do texto.

Segurança

Deve ser claro que o requisito mínimo de segurança é que qualquer adversário com acesso ao texto-cifrado e conhecimento acerca dos algoritmos de encriptação e decriptação utilizados não seja capaz de recuperar o texto-plano. No entanto, outras propriedades são desejáveis:

- Deve ser difícil recuperar as mensagens-planas a partir do texto-cifrado para qualquer distribuição de probabilidade no espaço das mensagens-planas (assume-se que o adversário conhece essa distribuição, a probabilidade "a priori").
- Deve-ser difícil, também, recuperar "informação parcial" sobre mensagens-planas, ou seja, reduzir a incerteza a respeito da mensagem-plana.

Segurança por Obscuridade e Lei de Kerckhoff. Uma premissa fundamental em criptografia moderna é que os conjuntos M, C, K, $\{e_k : k \in K\}$ e $\{d_k : k \in K\}$ são de conhecimento público - a segurança do esquema deve residir inteiramente no par (e, d), que é a única coisa que deve ser mantida secreta. Esta premissa é conhecida como Lei de Kerckhoff.

(Em oposição à idéia acima, existe o controverso Princípio de Segurança por Obscuridade que procura ocultar detalhes como o projeto, a implementação e os algoritmos de comunicação para garantir a segurança. A experiência mostra que é bastante difícil manter secretos estes detalhes, de forma que os criptossistemas modernos não deveriam se basear neste princípio. A discussão entre as vantagens dos princípios de Kerckhoff e de Segurança por Obscuridade está fora do escopo deste trabalho, de forma que não a conduziremos aqui. Os criptossistemas desta dissertação serão

sempre analisados à luz dos conceitos modernos de criptografia, e, particularmente, da Lei de Kerckhoff.)

Criptanálise

Em termos de criptanálise, existem diferentes níveis de ataques aos criptossistemas:

1. "Ciphertext-only". O criptanalista possui um conjunto de mensagens-cifradas $y_1, ..., y_n \in C$. Este é o tipo de ataque mais elementar, em que o criptanalista simplesmente obtém acesso ao canal de comunicação e "observa" as mensagens-cifradas trocadas, sem, no entanto, saber o significado de cada uma delas (ou seja, a mensagem-plana correspondente).

2. "Known-plaintext". O criptanalista possui um conjunto de mensagens-planas $x_1, ..., x_n \in P$ e as mensagens-cifradas $y_1, ..., y_n \in C$ correspondentes a cada mensagem-plana.

3. "Chosen-plaintext". O oponente pode escolher um conjunto de mensagens-planas $x_1, ..., x_n \in P$ e obter as mensagens-cifradas $y_1, ..., y_n \in C$ correspondentes. (Essa é a situação em que o criptoanalista obtém acesso temporário à "máquina de encriptação".)

4. "Chosen-cyphertext". O oponente pode escolher um conjunto de mensagens-cifradas $y_1, ..., y_n \in C$ e obter as mensagens-planas $x_1, ..., x_n \in P$ correspondentes. (Essa é a situação em que o criptoanalista obtém acesso temporário à "máquina de decriptação".)

Em cada um destes ataques, o objetivo do criptoanalista é:

- identificar ou reduzir a incerteza sobre a chave k; ou

- determinar ou reduzir a incerteza sobre a mensagem-plana correspondente a determinada(s) mensagem(ns) cifrada(s)

Observe, ainda, que a determinação da chave k reduz a zero a incerteza sobre as mensagens-cifradas. No entanto, é possível reduzir a zero a incerteza sobre determinada mensagem cifrada c sem determinar unicamente a chave. Basta, para isso, reduzir o conjunto das "chaves possíveis" a um conjunto $\tilde{K}$ tal que $\forall k \in \tilde{K}, d_k(c) = p$ e certamente a mensagem-plana correspondente a c será p. (Observe que a discussão anterior se refere ao caso de criptossistemas de chave simétrica, onde a posse de qualquer uma das chaves de encriptação ou decriptação implica o conhecimento sobre a outra. O foco desta dissertação será nesse tipo de criptossistema, de forma que os criptossistemas de chave pública serão discutidos, em alguns momentos, apenas com fins de contextualização.)

Os últimos dois ataques podem parecer pouco razoáveis à primeira vista, mas são bastante comuns quando o algoritmo criptográfico, cuja chave é fixada por um fabricante e desconhecida pelo criptanalista, está inserido em um dispositivo livremente manipulável.

Cifras, Códigos e Esteganografia

Os conceitos de cifra, esteganografia e código são bastante relacionados. Todos se destinam à proteção da informação. As cifras consistem em métodos destinados a esconder a informação presente em mensagens, através de transformações que introduzem um alto grau de "confusão" na mensagem a ser transmitida. A esteganografia, por sua vez, tenta esconder a própria existência da mensagem, através de sua inserção em textos com sentido ou em imagens. Um código é uma espécie de "nova linguagem" que é combinada entre membros de um grupo que deseja estabelecer uma comunicação

segura. A principal característica de um código é a inexistência de chaves, de forma que a regra de comunicação é unica. Os exemplos variam desde os mais simples, como o código Morse, até os mais complexos, como é o caso de certos códigos militares.

Criptologia: Definição

A criptologia é o estudo das técnicas matemáticas relacionadas aos aspectos de segurança da informação, particularmente sua integridade, confidencialidade e autenticidade. A criptologia pode ser vista como composta de "criptografia", que é o conjunto de técnicas e conhecimentos para a construção de sistemas de segurança da informação (criptossistemas), e "criptoanálise" (ou "criptanálise"), que é é o estudo das técnicas matemáticas para tentar "derrubar" ou "quebrar" criptossistemas.

1.1.3 Cifradores de Bloco

Existem duas classes de criptossistemas comumente descritos: os cifradores de bloco e os de stream. Um cifrador de bloco é um esquema de encriptação que quebra o texto plano em "blocos" de tamanho fixo e encripta um bloco de cada vez. Um cifrador de stream é uma espécie de cifrador de bloco de comprimento igual a 1, ou seja, os símbolos são encriptados um a um. A própria distinção entre cifradores de bloco e de stream não é muito formal, residindo mais em aspectos práticos que no rigor matemático. Duas classes importantes de cifradores de bloco, e que formam a base para cifradores complexos, são as cifras de substituição e as cifras de transposição, estudadas a seguir. Cifras de substituição são cifradores de bloco que substituem grupos de símbolos (possivelmente unitários) por outros grupos de símbolos. Cifras de transposição modificam as posições dos símbolos de uma mensagem. (De forma geral, nos criptossistemas de bloco, o espaço das mensagens-planas é o mesmo que o

das mensagens-cifradas. Geralmente nos referiremos a este espaço por M.)

Cifras de Substituição Simples

Seja A um alfabeto de q símbolos e M o conjunto de todas as seqüências de símbolos de comprimento t em A. Defina o espaço das chaves K como sendo o conjunto das transformações bijetivas $k : A \to A$. Então, cada transformação de encriptação $e_k \in E$ é definida por

$$e_k(m) = (k(a_1)k(a_2)...k(a_t)) = (c_1c_2...c_t) = c,$$

onde $m = (a_1a_2...a_t) \in M$. Em outras palavras, para cada símbolo em um t-upla, substitua-o por outro símbolo de A, de acordo com uma bijeção $k : A \to A$. Para decriptar $c = (c_1c_2...c_t)$, aplique a inversa k^{-1} a cada caractere:

$$d_k(c) = (k^{-1}(c_1)k^{-1}(c_2)...k^{-1}(c_t)) = (a_1a_2...a_t) = m.$$

O criptossistema definido acima é chamado cifra de substituição simples ou cifra de substituição monoalfabética.

O número de cifras de substituição simples distintas é $q!$ e é independente do tamanho t do bloco. Na verdade, poderíamos ter definido a cifra de substituição de forma independente da idéia de blocos; o motivo pelo qual não o fizemos foi para facilitar a definição do conceito de composição de cifradores, a ser introduzido posteriormente.

A cifra de substituição, por si só, oferece segurança inadequada, mesmo possuindo um espaço de chaves grande. De fato, a freqüência relativa dos símbolos do texto plano é mantida no texto cifrado. Assim, o símbolo que aparece com maior freqüência no texto cifrado provavelmente corresponderá ao símbolo que se sabe, *a priori*, ser mais

freqüente na "linguagem" do texto plano (por exemplo, a letra "A" na lingua portuguesa e a letra "E" na inglesa). Através da observação de uma pequena quantidade de texto cifrado e conhecendo-se as probabilidades *a priori* de ocorrência de símbolos na linguagem do texto plano, o criptoanalista pode facilmente determinar a chave.

Cifras de Substituição Homofônica

A cada símbolo $a \in \mathcal{A}$, associe um conjunto $H(a)$ de seqüências de símbolos de comprimento t, com a restrição de que os conjuntos $H(a)$, $a \in \mathcal{A}$, sejam disjuntos dois a dois. A cifra de substituição homofônica substitui cada símbolo no texto plano por um dos elementos de $H(a)$, escolhido aleatoriamente. A desencriptação é feita pela substituição dos símbolos do texto cifrado pelos símbolos correspondentes em $\mathcal{A}$.

O cifrador homofônico pode ser usado para alterar a freqüência relativa dos símbolos no texto cifrado, tornando-a mais uniforme (isto pode ser feito associando conjuntos $H(a)$ maiores aos símbolos mais freqüentes). O preço a se pagar por essa uniformização é o aumento do tamanho do texto cifrado.

Cifra de Substituição Polialfabética

Cifras de substituição polialfabética são simplesmente uma generalização das cifras de substituição simples em que se faz a substituição de grupos de símbolos por outros grupos de símbolos.

Cifras de Transposição

como já mencionamos, além das cifras de substituição (três das quais foram mostradas anteriormente), a outra classe básica de cifras de bloco são as cifras de transposição. Uma cifra de transposição simples faz a permutação dos símbolos em um bloco. Considere um esquema de encriptação de bloco de comprimento t. Seja $\mathcal{K}$ o conjunto

das permutações do conjunto $\{1, 2, ..., t\}$. Para cada $e \in K$, a função de encriptação é definida por

$$E_e(m) = (a_{e(1)}a_{e(2)}...a_{e(t)}),$$

onde $m = (a_1a_2...a_t) \in \mathcal{M}$. O conjunto de todas as tranformações deste tipo é uma cifra de transposição simples. A chave de desencriptação correspondente a e é a permutação inversa $d = e^{-1}$. Para decriptar $c = (c_1c_2...c_t)$ computa-se $D_d(c) = (c_{d(1)}c_{d(2)}...c_{d(t)})$.

A cifra de transposição simples preserva o número de símbolos de cada tipo no bloco, sendo uma cifra de fácil criptoanálise.

Composição de Cifradores / Redes de Substituição-Permutação

Cifradores simples de substituição e de transposição não fornecem um grau elevado de segurança. No entanto, através da combinação desses dois tipos de transformações é possível contruir fortes cifradores. A maioria dos cifradores de chave simétrica é baseada na composição de cifradores (também chamado de produto de cifradores).

Redes de Substituição-Permutação. Uma SPN - "Substitution-Permutation Network" - é uma estrutura simples, mas que é a base para alguns dos principais cifradores de bloco da atualidade. A encriptação é alcançada após repetidas aplicações de "rounds" compostos de três etapas. A primeira etapa é a **substituição** de grupos de símbolos por outros grupos de símbolos, de acordo com regras predeterminadas. A segunda etapa é a **permutação** de símbolos (troca de posições). Na terceira etapa ocorre a aplicação de alguma **função dependente da chave**, como um XOR (uma soma "módulo 2" efetuada para cada par de bits contendo um bit de cada operando) com parte da chave (esta etapa é chamada de "key mixing").

1.1.4 Cifradores de "Stream"

Cifradores de "stream" são uma classe importante de esquemas de criptografia de chave simétrica. São, de certa forma, cifradores de bloco de comprimento igual à unidade, consistindo em uma extensão simples à nossa definição de criptossistema. Como nos cifradores de "stream", o comprimento de cada "bloco" é muito pequeno, a aplicação da mesma transformação de encriptação a cada bloco levaria a uma cifra muito simples. Para facilitar a visualização, no caso extremo, em que o bloco é formado de um único bit, haveria apenas dois mapeamentos possíveis para cada bit (0 ou 1) e a mensagem-cifrada seria um dos dois casos a seguir: ou exatamente a mensagem-plana ou a mensagem composta pela troca de cada bit 1 por um bit 0 e de cada bit zero por um bit um.

Para que a mensagem-cifrada seja mais complicada, gera-se uma seqüência de novas chaves a partir da chave original e cada caractere é encriptado de acordo com uma dessas chaves.

Cifradores de stream encriptam os caracteres de um texto plano um a um, em contraste com os cifradores de bloco que encriptam, a cada vez, um bloco de caracteres, através de uma transformação fixa. Os cifradores do tipo "stream" são mais apropriados em certas aplicações, geralmente aquelas nas quais os buffers são limitados ou quando os caracteres devem ser processados à medida em que chegam, para evitar atrasos na comunicação.

Cifradores de "stream" são comumente classificados como síncronos ou auto-sincronizantes.

(i) Cifradores síncronos:

No caso dos cifradores síncronos, a "keystream" é gerada de forma independente

do texto-plano:

$$\begin{cases} k_i = g(k_{i-1}) \\ c_i = h(k_i, m_i) \end{cases}$$

onde $k_0 = k$ é chave k utilizada, g é a função que produz a keystream e h é a função de saída que combina a keystream e o texto plano para produzir o texto cifrado. A maioria dos cifradores de "stream" propostos é do tipo aditivo, onde a função de saída h é a função XOR, ou seja, a "soma módulo 2" efetuada bit-a-bit.

(ii) Cifradores auto-sincronizantes

São cifradores em que a keystream é gerada em função da chave e de um número fixo de dígitos anteriores do texto cifrado:

$$\begin{cases} k_i = g(c_{i-t}, c_{i-t+1}, ..., c_i, k_0) \\ c_i = h(k_i, m_i). \end{cases}$$

Cifrador de Vernam, One-time Pad.

Um cifrador de Vernam é um cifrador definido no alfabeto $\mathcal{A} = \{0, 1\}$. Uma mensagem binária $m_1m_2m_3...m_t$ é operada através de uma keystream $k_1k_2k_3...k_t$ para produzir o texto cifrado $c_1c_2c_3...c_t$, onde $c_i = m_i + k_i \ (mod\ 2),\ 1 \leq 1 \leq t$. Se a chave é gerada aleatoriamente e nunca mais utilizada, o cifrador de Vernam é chamado de "one-time system" ou de "one-time pad". O one-time pad é um cifrador teoricamente inquebrável.

O cifrador de Vernam é incondicionalmente seguro contra um ataque "ciphertext-only", porém, uma desvantagem do "one-time pad" é que a chave deve ser tão longa quanto o texto plano, o que dificulta a distribuição e o gerenciamento de chaves. Isto motiva o projeto de cifradores em que a keystream é gerada de forma pseudo-aleatória a partir de uma chave secreta menor. Apesar de, aparentemente, ser de difícil utilização, o one-time pad chegou a ser usado para comunicações ultra-secretas

durante a guerra fria, onde agentes secretos faziam o transporte das chaves (seqüências de símbolos). Estas chaves eram usadas apenas uma vez e descartadas.

1.1.5 Criptografia de Chave Pública

Os esquemas de criptografia estudados até o momento possuem a propriedade de que dada uma das funções de encriptação ou de decriptação, é fácil determinar a outra. Na abordagem da criptografia de chave pública, por outro lado, utilizam-se pares de transformações de encriptação/decriptação (e_k, d_k) tais que a partir de e_k, é difícil determinar d_k. Interessantes aplicações surgem, nesse caso. A principal aplicação é uma abordagem diferente de comunicação. No caso da criptografia de chave pública, podemos pensar a chave como sendo composta de duas partes, $k = (k_e, k_d$, onde k_e determina a função de encriptação e k_d, a função de decriptação. Assim, o transmissor não precisa conhecer "toda a chave", mas apenas a parte k_e que determina a função de encriptação d_k. Dessa forma, uma vez encriptada a mensagem, apenas o receptor (possuidor de k_d) é capaz de decriptá-la, mesmo considerando que k_e é divulgada publicamente.

Exemplo: Algoritmo RSA. A seguir apresentamos um exemplo mais prático de criptografia de chave pública, bastante utilizado nos dias de hoje.

O sistema RSA foi desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman. Neste sistema um usuário escolhe um par de números primos tão grande que fatorar o produto entre eles é uma tarefa que que não é viável, consideradas as capacidades computacionais existentes.

Sejam p e q esses primos. O usuário computa o produto $n = pq$. Esse produto n é chamado de módulo. Então o usuário escolhe um número e, o expoente público, menor que n e sem fatores comuns com $(p-1)(q-1)$. Um outro número, d, chamado

expoente privado, é, então, calculado pelo usuário, com a propriedade de que $(ed-1)$ é divisível por $(p-1)(q-1)$. A chave pública é o par (n, e) e a chave privada é o par (n, d). Os primos p e q podem ser destruídos ou mantidos secretos.

É virtualmente impossível obter d a partir de n e e. No entanto, é fácil obter d se conhecermos p e q. Assim, a segurança do RSA se baseia no fato de que fatorar é "difícil". Os seguintes estágios são seguidos para se enviar uma mensagem:

1. O receptor, M, distribui sua chave pública.

2. O transmissor, F, compõe um texto m e usa a chave pública de M para encriptar a mensagem e gerar c, onde $c = m^e \ (mod\ n)$.

3. F envia c a M.

4. M decifra c usando d e n: $m = c^d \ (mod\ n)$.

Em relação às propriedades dos esquemas de criptografia de chave pública e o de chave privada, podemos observar algumas diferenças. As diferenças mais visíveis são o tamanho da chave e a velocidade de encriptação. Enquanto os esquemas de chave simétrica possuem chaves relativamente pequenas e elevadas velocidades de encriptação, os esquemas de chave pública possuem chaves grandes e são mais lentos.

A principal diferença entre a criptografia de chave pública e a de chave privada é relacionada ao gerenciamento das chaves; enquanto na primeira é necessário um par de chaves para cada par de usuários que quer se comunicar, devendo ambas ficar secretas, na última existe um par de chaves para cada usuário, sendo que uma destas chaves é divulgada. Na verdade as duas abordagens possuem vantagens complementares. Os esquemas de criptografia atuais exploram as forças de cada uma.

1.1.6 Mais sobre Segurança

Resistência a Ataques

Uma forma prática de avaliar a segurança de um criptossistema é testá-lo contra uma série de ataques conhecidos. O criptossistema será, então, classificado, de acordo com a sua resistência às classes de ataques.

Podemos classificar os ataque a esquemas de critografia em ataques ativos e passivos. Em um ataque passivo, o adversário apenas monitora o canal de comunicação. No ataque ativo, o adversário tenta atacar a integridade da mensagem, inserindo, modificando ou apagando seus símbolos.

O ataque "ciphertext-only" é um ataque passivo onde o criptoanalista tem acesso somente às mensagens criptografadas (uma "stream" de bits) do criptossistema. O criptoanalista tenta achar regularidades estatísticas na "stream" criptografada, desvios da aleatoriedade que podem indicar a natureza da chave. A maioria dos criptossistemas (exceto os muito ingênuos) produz texto-cifrado com um alto grau de aleatoriedade, de modo que um criptossistema vulnerável a este tipo de ataque é considerado muito fraco.

Um modelo mais forte de ataque passivo é o "known-plaintext", onde o criptoanalista tem acesso a pares de mensagens cifradas e os textos-planos que as deram origem. Atualmente, considera-se criptossistemas suscetíveis a este tipo de ataque como sendo fracos e desinteressantes.

No modelo de ataques ativos, o criptoanalista pode "escolher" mensagens quaisquer e ter acesso às mensagens criptografadas ("chosen-plaintext") ou, ao contrário, escolher mensagens criptografadas e ter acesso aos textos-planos que originam as mensagens criptografadas escolhidas ("chosen-ciphertext"). Pelos padrões atuais, um

bom criptossistema deve ser resistente a ataques que permitem ao criptoanalista escolher tanto o texto-plano quanto a mensagem criptografada, segundo qualquer estratégia à sua escolha. Além disso, o criptossistema deve resistir aos ataques de criptanálise linear e diferencial, já considerados "ataques-padrão" e descritos brevemente na seqüência.

Criptanálise Diferencial

A criptanálise diferencial foi desenvolvida por Biham e Shamir [**?**] em 1993 e é um ataque do tipo chosen-plaintext. Neste ataque, são analisadas as diferenças entre pares de mensagens-planas e entre os pares de mensagens-cifradas correspondentes. Estas diferenças podem ser utilizadas para determinar as possíveis chaves e localizar a chave mais provável. Geralmente, as diferenças são definidas como um XOR das mensagens. O objetivo da criptanálise diferencial é reduzir o número de testes quando comparada com um ataque de força-bruta.

A criptanálise diferencial explora a alta probabilidade de ocorrência de certas "diferenças" nas mensagens-planas e nas mensagens cifradas. Por exemplo, considere um sistema com entrada $X = (X_1, ..., X_n)$ e saída $Y = (Y_1, ..., Y_n)$. Sejam X' e X'' duas entradas e Y' e Y'' suas saídas correspondentes. A "diferença" da entrada" será dada por $\Delta X = XOR(X', X'')$ e a "diferença" da saída" será dada por $\Delta Y = XOR(Y', Y'')$. Em um cifrador ideal, a probabilidade de que uma determinada diferença de saída ΔY ocorra para uma dada diferença de entrada ΔX é $1/2^n$, onde n é o número de bits de X. A criptanálise diferencial explora o cenário onde uma diferença particular de saída ocorre com relativa alta probabilidade para uma diferença particular de entrada. Refere-se ao par $(\Delta X, \Delta Y)$ por "diferencial".

A "probabilidade de aproximação diferencial" de um dado mapa f, DP_f, é definida

por

$$DP_f = \max_{\Delta X \neq 0, \Delta Y \neq 0} \left(\frac{\sharp\{x \in M | XOR(f(x), f(XOR(x, \Delta X))) = \Delta Y\}}{2^n} \right),$$

onde 2^n é a cardinalidade do espaço das mensagens M. Assim, DP_f é uma espécie de medida da difusão de f, ou de sua sensibilidade às condições iniciais. Quanto menor o valor de DP_f, melhores suas propriedades criptográficas.

Criptanálise Linear

A criptanálise linear foi desenvolvida por Matsui [**?**] em 1994. É um ataque do tipo known-plaintext cujo objetivo é construir uma expressão linear aproximada do cifrador de bloco em estudo. A criptanálise linear procura tirar vantagem de expressões lineares envolvendo bits das entradas e saídas de um cifrador. A idéia básica da criptanálise linear é tentar aproximar a operação de um cifrador através de uma expressão dada com operações módulo 2 (ou seja, XOR, representada aqui pelo operador binário $\oplus$). São expressões da forma

$$X_{i_1} \oplus X_{i_2} \oplus ... \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus ... \oplus Y_{j_v} = 0,$$

onde X_α representa o α-ésimo bit da entrada X e Y_β representa o β-ésimo bit da saída Y.

A abordagem utilizada pela criptanálise linear é determinar expressões da forma acima para as quais haja "alta" ou "baixa" probabilidade de ocorrência. Se um cifrador mostra tendência para uma expressão como a acima valer com alta probabilidade ou não valer com alta probabilidade, isto é uma evidência de propriedades aleatórias fracas (se $u+v$ bits aleatórios fossem inseridos na expressão acima, a probabilidade de ela ser verdadeira seria de 1/2). A criptanálise linear explora o desvio da probabilidade 1/2 e quanto maior for este desvio, melhor para o criptoanalista.

Modelos para a avaliação da Segurança

A medida mais severa de segurança é uma medida com origem na Teoria da Informação: "segurança incondicional". Considera-se um adversário que possui recursos computacionais ilimitados e pergunta-se se existe ou não informação disponível suficiente para se derrotar o sistema. Num sistema com segurança incondicional, a incerteza com relação ao texto plano após a observação de um texto cifrado deve ser igual à incerteza "a priori" com relação ao texto plano, ou seja, a observação do texto cifrado não fornece nenhuma informação ao adversário.

Uma condição necessária para um esquema de chave simétrica ser incondicionalmente seguro é que a chave seja pelo menos tão grande quanto a mensagem. O "one-time pad" é um exemplo. Em geral os esquema de criptografia não oferecem segurança incondicional, e à medida que se observa texto cifrado, a incerteza sobre o texto plano decresce. Esquemas de chave pública não podem ser incondicionalmente seguros, já que, dados uma chave pública e um texto cifrado, para descobrir o texto plano correspondente bastaria encriptar todas as possibilidades de texto plano até que uma delas coincidisse com o texto cifrado.

Um método criptográfico é dito de "segurança provável" se a dificuldade em "quebrá-lo" pode ser mostrada tão difícil quanto algum outro problema conhecido e supostamente difícil, como por exemplo a fatoração de inteiros ou a computação do logaritmo discreto.

"Segurança computacional" é a medida do esforço computacional necessário para, através do melhor método conhecido, derrotar o sistema. O sistema é dito computacionalmente seguro se a quantidade de recursos computacionais exigidos para derrotá-lo, usando a melhor técnica conhecida, excede os recursos que o adversário

por hipótese possui. O conceito também é referido como "segurança prática".

A segurança computacional é geralmente medida em termos da variação da complexidade do tempo (processamento) e espaço (memória) necessários para que a condução de determinado tipo de ataque seja bem-sucedida em relação à variação do tamanho da chave (ou outro parâmetro).

Segurança Perfeita

a segurança incondicional também é denominada "segurança perfeita". Considere o seguinte cenário. A e B desejam comunicar-se através de um canal inseguro, observado por Z. Z observa um texto-cifrado $c \in C$ e tenta obter alguma informação a respeito do texto-plano correspondente. Os textos planos são distribuídos de acordo com uma distribuição de probabilidade Pr_P. Além disso, a chave é escolhida de forma independente do texto a ser encriptado. As chaves estão distribuídas de acordo com uma distribuição de probabilidade Pr_K em K. As distribuições Pr_P e Pr_K induzem uma distribuição de probabilidade $Pr_{P\times K}$ em $P \times K$. Então, para cada texto-plano p e cada chave k, $Pr_{P\times K}(p,k) = Pr_P(p)Pr_K(k)$ é a probabilidade de termos o texto-plano p encriptado com a chave k, onde p e k são independentes.

$Pr_P(p)$ é a probabilidade de que o texto-plano p seja encriptado, enquanto $Pr_K(k)$ é a probabilidade de que a chave k seja utilizada. Seja c uma variável aleatória cuja distribuição é determinada pelo criptossistema utilizado. Então, $Pr_P(p|c)$ é a probabilidade de que p é encriptado dado que c é recebido. O observador Z sabe o texto-cifrado c e conhece a distribuição de probabilidade Pr_p, a chamada probabilidade "a priori" de ocorrência dos textos-planos, característica da linguagem ou código utilizado.

Lembramos que $C_k = e_k(P) = \{e_k(p) : p \in P\}$, ou seja, C_k é o conjunto das

possíveis mensagens cifradas. Então, para cada $c \in C$ teremos

$$Pr_C(c) = \sum_{\{k:c\in C_k\}} Pr_K(k)Pr_P(d_k(c)).$$

Observe, também, que para qualquer $c \in C$ e $p \in P$, podemos calcular a probabilidade condicional $Pr(c|p)$:

$$Pr_C(c|p) = \sum_{\{k:p=d_k(c)\}} Pr_K(k).$$

É possível, assim, calcular a probabilidade condicional $Pr_P(p|c)$ usando o teorema de Bayes:

$$Pr_P(p|c) = \frac{Pr_P(p)Pr_C(c|p)}{Pr_C(c)}.$$

Definição: Um criptossistema (P, C, K, E, D) provê "segurança perfeita" se e somente se $Pr_P(p|c) = Pr_P(p)$ para todo $p \in P$ e para todo $c \in C$.

Ou seja, a probabilidade de $p \in P$ não muda após a observação de um texto cifrado $c \in C$; qualquer que seja c, ele não irá "fornecer informação" sobre o criptossistema.

Exemplo de criptossistema que não oferece Segurança Perfeita

O seguinte exemplo de criptossistema não provê segurança perfeita. Considere P, C e K dados da seguinte forma:

$$P = \{0, 1\}, \text{ onde } Pr_P(0) = \frac{1}{4} \text{ e } Pr_P(1) = \frac{3}{4};$$

$$K = \{A, B\}, \text{ onde } Pr_K(A) = \frac{1}{4} \text{ e } Pr_K(B) = \frac{3}{4};$$

$$C = \{a, b\}.$$

E sejam as funções de encriptação dadas por $e_A(0) = a$, $e_A(1) = b$, $e_B(0) = b$, $e_A(1) = b$.

Então, a probabilidade de que o texto-cifrado a ocorra é

$$Pr_C(a) = Pr_{P\times K}(0, A) + Pr_{P\times K}(1, B) = Pr_P(0)Pr_K(A) + Pr_P(1)Pr_K(B) = \frac{5}{8}.$$

A probabilidade de que o texto-cifrado b ocorra é

$$Pr_C(b) = Pr_{P\times K}(1, A) + Pr_{P\times K}(0, B) = Pr_P(1)Pr_K(A) + Pr_P(0)_K Pr(B) = \frac{3}{8}.$$

Então, para cada par $(p, c) \in P \times C$, a probabilidade condicional $Pr(p|c)$ é:

$$Pr(0|a) = \frac{Pr_{P\times K}(0, A)}{Pr_C(a)} = \frac{1/16}{5/8} = \frac{1}{10};$$

$$Pr(0|b) = \frac{Pr_{P\times K}(0, B)}{Pr_C(b)} = \frac{3/16}{3/8} = \frac{1}{2};$$

$$Pr(1|a) = \frac{Pr_{P\times K}(1, B)}{Pr_C(a)} = \frac{9/16}{5/8} = \frac{9}{10};$$

$$Pr(1|b) = \frac{Pr_{P\times K}(1, A)}{Pr_C(b)} = \frac{3/16}{3/8} = \frac{1}{2};$$

Em particular, observamos que $Pr_P(0) = \frac{1}{4} \neq \frac{1}{10} = Pr_P(0|a)$ e o criptossistema não provê segurança perfeita: se o observador Z detecta um texto-cifrado a, ele pode ter "quase certeza" de que o texto-plano correspondente é um 1.

O Teorema de Shannon

Vamos, agora, investigar a "segurança perfeita" de uma forma geral. Primeiro, observe que, usando o teorema de Bayes, a condição $Pr_P(p|c) = Pr_P(p)$ para todo $p \in P$, $c \in C$ é equivalente a $Pr_C(c|p) = Pr_C(c)$ para todo $p \in P$, $c \in C$. Agora, façamos a razoável hipótese de que $Pr_C(c) > 0$ para cada $c \in C$ (caso contrário, a mensagem-cifrada nunca é utilizada e pode ser excluída de C). Escolha algum $p \in P$. Para cada $c \in C$, teremos $Pr_C(c|p) = Pr_C(c) > 0$. Logo, para cada $c \in C$ deve existir ao menos uma chave k tal que $e_k(p) = c$. Segue que $\#K \geq \#C$. Além disso,

devemos ter pelo menos $\#C \geq \#P$, pois cada regra de codificação é injetiva. Nesta dissertação, estamos nos focando em criptossistemas em que cada regra de codificação é bijetiva, e no caso em que $\#K = \#C = \#P$ temos uma interessante caracterização de sistemas perfeitos. O seguinte teorema foi desenvolvido por Shannon [3] em 1949 e caracteriza criptossistemas que fornecem segurança perfeita.

Teorema: Seja $S = (P, C, K, E, D)$ um criptossistema com $\#K = \#C = \#P$ e $Pr(p) > 0$ para cada $p \in P$. Então, S fornece segurança perfeita se e somente se

(1) Pr_K é uma distribuição uniforme, e

(2) para cada $p \in P$ e para cada $c \in C$ existe uma única chave $k \in K$ com $E_k(p) = c$.

Dem.: Assuma que S oferece segurança perfeita. Mostraremos que (1) e (2) são cumpridos.

(2): Como observamos anteriormente, para cada $p \in P$ e para cada $c \in C$ deve existir pelo menos uma chave k tal que $e_k(p) = c$. Então:

$$\#C = \#\{e_k(p) : k \in K\} \leq \#K.$$

Mas estamos assumindo que $\#K = \#C$. Logo, $\#\{e_k(p) : k \in K\} = \#K$. Assim, não existem duas chaves distintas k_1 e k_2 tais que $e_{k_1}(p) = e_{k_2}(p) = c$. Dessa forma, mostramos que para cada $p \in P$ e para cada $c \in C$ existe exatamente uma chave $k \in K$ com $E_k(p) = c$.

(1): Escolha um texto-cifrado $c \in C$. Para $p \in P$, seja $k(p, c)$ a única chave k tal que $E_k(p) = c$. Temos, então, para cada $p \in P$ (teorema de Bayes):

$$Pr(p|c) = \frac{Pr_c(c|p)Pr_p(p)}{Pr_c(c)} = \frac{Pr_k(k(p,c))Pr_p(p)}{Pr_c(c)}.$$

Como S provê segurança perfeita, temos que $Pr(p|c) = Pr(p)$. Logo, pela equação

acima, $Pr_K(k(p)) = Pr_P(p)$, independentemente de p. Logo, as probabilidades $Pr_K(k)$ são iguais para todo $k \in K$.

Analogamente, suponha que as condições 1 e 2 valem. Seja $k = k(p, c)$ a única chave que satisfaz $E_k(p) = c$. Usando o teorema de Bayes,

$$Pr_P(p|c) = \frac{Pr_P(p)Pr_C(c|p)}{Pr_C(c)} = \frac{Pr_P(p)Pr_K(k(p,c))}{\sum_{q \in P} Pr_P(q)Pr_K(k(q,c))}.$$

Como todas as chaves estão uniformemente distribuídas, segue que

$$Pr_K(k(q,c)) = \frac{1}{\#K}.$$

Além disso,

$$\sum_{q \in P} Pr_P(q)Pr_K(k(q,c)) = \frac{\sum_{q \in P} Pr_P(q)}{\#K} = \frac{1}{\#K}.$$

Substituindo na equação de $Pr_P(p|c)$, obtemos que $Pr_P(p|c) = Pr_P(p)$ e S oferece segurança perfeita.

O one-time pad

O criptossistema de Vernam descrito anteriormente e denominado "one-time pad" oferece segurança perfeita. Como vimos, nesse criptossistema $P = K = C = \{0,1\}^n$ para algum $n \in \mathbb{N}$. Para $k \in K$, defina as funções de encriptação, $E_k : \{0,1\}^n \to \{0,1\}^n$, e de decriptação, $D_k : \{0,1\}^n \to \{0,1\}^n$, como

$$E_k(p) = p + k \ (mod\ 2) \text{ e } D_k(c) = c + k \ (mod\ 2),$$

onde as chaves são distribuídas uniformemente em $\{0,1\}^n$. Lembramos que a cada novo texto-plano, uma nova chave deve ser selecionada.

Pelo teorema de Shannon, o one-time pad oferece segurança perfeita, já que para cada texto-plano $p \in P$ e para cada texto-cifrado $c \in C$, existe uma única chave $k \in K$ com $c = p \oplus k$, a saber, $k = c \oplus p$.

1.2 Cifradores Caóticos Digitais

Nesta seção faremos uma análise mais detalhada de alguns cifradores caóticos digitais desenvolvidos desde a década de 1980. Analisaremos exemplos de criptossistemas fracos (e como eles foram quebrados) e também de esquemas promissores de criptografia. O primeiro artigo [11] em que um sistema caótico foi explicitamente utilizado na construção de um cifrador foi publicado em 1989 onde o autor sugere um cifrador de stream baseado em um mapeamento caótico unidimensional. (Cabe observar que em 1985, Wolfram [9] apresenta uma proposta de cifrador baseado no uso de autômatos celulares, mas que não teve muito impacto na área da criptografia.) Desde então inúmeros esquemas têm sido propostos para aplicações de sistemas caóticos ao projeto de cifradores digitais.

Existem, basicamente, dois métodos principais para se projetar cifradores caóticos digitais:

1. Uso de sistemas caóticos para a geração de seqüências de números pseudo-aleatórios, os quais irão mascarar o texto plano;

2. uso do texto plano e/ou chave secreta como condição inicial e/ou parâmetro de um sistema dinâmico, iterando-o de forma a obter o texto cifrado.

Em ambos os casos, tanto o transmissor quanto o receptor têm acesso ao mesmo sistema caótico.

O primeiro método geralmente corresponde a cifradores de stream, enquanto o segundo corresponde a cifradores de bloco. Além desses dois métodos principais, outras abordagens podem ser encontradas na seção 2.5 desta dissertação.

1.2.1 Cifradores Baseados em Geradores de Números Pseudo-Aleatórios

Devido às órbitas pseudo-aleatórias "imprevisíveis" geradas pelos sitemas caóticos, muitos pesquisadores se dedicaram ao desenvolvimento de PRNG (pseudo random number generator - geradores de números pseudo-aleatórios) baseados nestes sistemas. O núcleo dos principais cifradores caóticos de stream são PRNGs cujas seqüências de saída são usadas para mascarar o texto plano.

Diversos sistemas caóticos foram usados para construir os geradores de números pseudo-aleatórios caóticos. Em [48] os autores discutem a combinação de sistemas caóticos baseados no mapeamento logístico:

$$\begin{cases} x_n = 4\lambda x_{n-1}(1 - x_{n-1}) \\ x'_n = 4\lambda x'_{n-1}(1 - x'_{n-1}) \\ c_n = XOR(XOR(x_n, x'_n), p_n) \end{cases}$$

onde XOR representa a operação "ou-exclusivo" (ou "soma módulo 2) efetuada bit-a-bit, p_n é o n-ézimo bit da mensagem-plana e c_n é o n-ézimo bit da mensagem-cifrada gerada. Observamos, ainda, que o parâmetro λ, assim como as condições iniciais x_0 e x'_0 farão parte da chave secreta. No contexto de cifradores de "stream" síncronos (ver página 16), temos $k_n = (x_n, x'_n, \lambda)$, $n = 0, 1, 2, ...$, $g(k) = (4\lambda x(1-x), 4\lambda x'(1-x'), \lambda)$, $h(k, p) = XOR(XOR(x, x'), p)$.

Os autores fazem criptoanálise diferencial, teste de Chi-quadrado (um teste de aleatoriedade descrito em [7]), simulações de ataque (força-bruta e texto-plano) e comparam o método com três cifradores populares, apresentando resultados que indicam as boas possibilidades de aplicação da abordagem.

Já em [13], os autores utilizam amostragens não uniformes em circuitos DPLL (digital phase-locked loop) operando em regime caótico. O sinal de entrada é definido

por $s(t) = h(\omega_1 t + \theta_0)$, onde $h(\cdot)$ é uma função de período 2π. O sinal de entrada $s(t)$ terá, então, freqüência ω_1 e ângulo de fase inicial θ_0. A amostragem é determinada por uma onda quadrada de saída do VFO - variable frequency oscillator - no tempo t_n. A saída do "bloco de amostragem" será $s_n = h(\omega_1 t_n + \theta_0)$ e poderá ser uma corrente, tensão, palavra binária etc, dependendo do tipo de VFO. O VFO consiste em um controle de entrada que seleciona o período do oscilador, $T_{n+1} = t_{n+1} - t_n = g(s_n)$, e uma saída de onda quadrada.

Em outros trabalhos, verifica-se, ainda, a construção de geradores de números pseudo-aleatórios a partir do atrator de Hénon [18] e do mapa de Chebyshev [25].

1.2.2 Cifrador de Stream de Shujun et al.

Shujun et al. [46] propõe o uso de pares de sistemas caóticos para a geração de números (bits) pseudo-aleatórios (Couple Chaotic Systems Based Pseudo Random Bit Generator, CCS-PRBG). Neste esquema, a saída do gerador de bits depende da comparação entre duas órbitas caóticas.

Considere dois mapas caóticos unidimensionais $f_1(x_1, p_1)$ e $f_2(x_2, p_2)$: $x_1(i+1) = f_1(x_1(i), p_1)$, $x_2(i+1) = f_2(x_2(i), p_2)$, onde p_1 e p_2 são parâmetros de controle, $x_1(0)$ e $x_2(0)$ são condições iniciais e $x_1(i)$ e $x_2(i)$ denotam as órbitas.

Shujun define uma seqüência pseudo-aleatória de bits que compara a relação entre $x_1(i)$ e $x_2(i)$. O problema com a definição de Shujun é que a função não está definida para o caso em que $x_1(i) = x_2(i)$. Faremos uma pequena modificação na notação de Shujun de forma a melhorar seu rigor matemático.

Defina uma seqüência pseudo-aleatória de bits dada por $k_i = k(i) = g(x_1(i), x_2(i))$,

onde

$$g(x_1, x_2) = \begin{cases} 1 \text{ se } (x_1 > x_2) \\ -1 \text{ se } x_1 = x_2 \\ 0 \text{ se } (x_1 < x_2). \end{cases}$$

Então, a a seqüência de bits definida no cifrador de Shujun é a subseqüência formada pelos elementos não-negativos de k_i, ou seja, $k_{i_j}|k(i_j) \geq 0$.

Segundo Shujun, o gerador de bits acima terá boas propriedades criptográficas se os seguintes requisitos forem satisfeitos:

R1) $f_1(x_1, p_1)$ e $f_2(x_2, p_2)$ são sobrejetivas no mesmo intervalo $I = [a, b]$;

R2) $f_1(x_1, p_1)$ e $f_2(x_2, p_2)$ são ergódicos em $I = [a, b]$;

R3) Uma das seguintes condições é valida: $f_1(x) = f_2(x) = f(x)$ ou $f_1(x)$ e $f_2(x)$ são simétricos pares em relação a $x = (a + b)/2$;

R4) $x_1(i)$ e $x_2(i)$ são assintoticamente independentes (quando $i \to \infty$).

O CCS-PRBG pode ser visto como um gerador caótico de números aleatórios onde o threshold é variável com o tempo. Observe que a seqüência $\{k(i)\}$ gerada pelo CCS-PRBG é balanceada em $\{0, 1\}$. Se os dois mapas caóticos utilizados satisfazem os requisitos R1-R4, então $P\{k(i) = 0\} = P\{k(i) = 1\}$, conforme mostramos abaixo

Como $f_1(x_1, p_1)$ e $f_2(x_2, p_2)$ são ergódicos em $I = [a, b]$ (R2), as órbitas geradas para quase todo ponto irão levar às mesmas funções de distribuição $f_1(x)$ e $f_2(x)$. De R4, sabemos que as órbitas $x_1(i)$ e $x_2(i)$ são assintoticamente independentes, então, as probabilidades de que $x_1 > x_2$ e $x_1 < x_2$ quando $i \to \infty$ serão:

$$P\{x_1 < x_2\} = \int_a^b \int_a^x f_1(x) f_2(y) dy dx,$$
$$P\{x_1 > x_2\} = \int_a^b \int_a^x f_2(x) f_1(y) dy dx.$$

Agora, basta mostrar que as duas probabilidades serão iguais quando valer o requisito R3. Se $f_1(x) = f_2(x) = f(x)$, é claro que as duas integrais serão idênticas. Considere,

então, o caso em que $f_1(x)$ e $f_2(x)$ são simétricos em relação a $x = (a+b)/2$.Observe que

$$\begin{aligned} f_1(x) &= f_1\left(x - \frac{a+b}{2} + \frac{a+b}{2}\right), \\ &= f_1\left(\frac{a+b}{2} - \left(x - \frac{a+b}{2}\right)\right), \\ &= f_1\left(\frac{a+b}{2} - x + \frac{a+b}{2}\right), \\ &= f_1(a+b-x), \end{aligned}$$

e, analogamente

$$f_2(x) = f_2(a+b-x).$$

Então,

$$\begin{aligned} P(x_1 < x_2) &= \int_a^b \int_a^x f_1(x) f_2(y) dy dx, \\ &= \int_a^b \int_a^x f_1(a+b-x) f_2(a+b-y) dy dx. \end{aligned}$$

Fazendo a mudança de variáveis

$$\tilde{x} = a+b-x, \quad d\tilde{x} = -dx,$$

$$\tilde{y} = a+b-y, \quad d\tilde{y} = -dy.$$

Obtemos

$$\begin{aligned} P(x_1 < x_2) &= -\int_a^b \int_b^{a+b-x} f_1(a+b-x) f_2(\tilde{y}) d\tilde{y} dx, \\ &= \int_b^a \int_b^{\tilde{x}} f_1(\tilde{x}) f_2(\tilde{y}) d\tilde{y} d\tilde{x}, \\ &= \int_a^b \int_{\tilde{x}}^b f_1(\tilde{x}) f_2(\tilde{y}) d\tilde{y} d\tilde{x}, \\ &= \int_a^b \int_a^{\tilde{x}} f_1(\tilde{y}) f_2(\tilde{x}) d\tilde{y} d\tilde{x}, \\ &= P(x_1 > x_2), \end{aligned}$$

e a afirmação está demonstrada.

1.2.3 Cifrador de Bloco de Habutsu et al.

Este criptossistema foi proposto na conferência Eurocript'1991 [20]. O sistema é baseado na iteração de um mapeamento caótico onde a mensagem-plana de 64 bits e encriptada em uma mensagem-crifrada de 147 bits. O sistema pode ser quebrado com ataques chosen-ciphertext e known-plaintext, conforme foi mostrado em [19].

Descrição do Criptossistema

Habutsu propõe um criptossistema de chave secreta que usa um mapa caótico unidimensional. No esquema, usa-se o parâmetro do mapa como chave secreta e codifica-se o texto-plano como um ponto no intervalo $[0, 1]$. A função de encriptação é dada por $G_e = g_{e_n} \circ g_{e_{n-1}} \circ ...g_{e_1}$, onde $e = (e_1, e_2, ..., e_{n-1}, e_n)$ é uma seqüência de bits (0 ou 1) que pode ser extraído da chave ou do próprio texto-plano (em seu artigo, Habutsu não deixa claro como selecionar essa seqüência). As funções $g_0 : [0, 1] \rightarrow [0, 1]$ e $g_1[0, 1] \rightarrow [0, 1]$ são definidas como se segue:

$$g_0(x) = ax,$$

$$g_1(x) = 1 - (1 - a)x + 1,$$

onde a é um parâmetro definido a partir da chave secreta e que varia no intervalo $(0, 1)$. A desencriptação é feita com a aplicação de F^n sobre o texto-cifrado, onde F é dada abaixo:

$$F(x) = \begin{cases} f_0(x) = \frac{x}{a} \text{ se } (0 \leq x \leq a), \\ f_1(x) = \frac{x-1}{a-1} \text{ se } (a < x \leq 1). \end{cases}$$

O criptossistema funciona da seguinte forma. Primeiro, escolhe-se uma chave secreta que definirá um valor para a, o parâmetro das funções definidas acima. O processo de encriptação funciona escolhendo-se como mensagem-plana um ponto $p \in (0, 1)$ e calculando-se a mensagem-cifrada $c = G_e(p)$. Novamente enfatizamos o fato

que Habutsu não deixa claro de onde obteremos a seqüência e (duas possibilidades são da chave secreta ou da própria mensagem-plana). Naturalmente, o processo de decriptação é dado pelo cálculo de $F^n(c) = F^n(G_e(p)) = p$.

Habustu sugere o uso de $n = 75$ iterações para encriptar mensagens-planas de 64 bits em mensagens cifradas de 147 bits.

Criptoanálise

Em [19], E. Biham demonstra ataques do tipo "chosen-ciphertext" e "known-plaintext" ao criptossistema de Habutsu. Para definir unicamente F^{-1}, Biham determina que a mensagem-plana seria composta por mais 75 "bits de escolha" após os 64 bits originais, os quais seriam utilizador para escolher entre f_1 e f_2.

Ataque chosen-ciphertext. Se todos os 75 bits da seqüência e forem escolhidos como zero, então a imagem das mensagens cifradas estará no intervalo $[0, a^{75}]$. Utilizando a precisão sugerida no trabalho de Habutsu, pode-se verificar que a^{75} estará no intervalo $(2^{-100}, 2^{-55})$. Assim, no intervalo $[0, a^{75}]$, toda mensagem cifrada C corresponderá à mensagem plana $C = p/a^{75}$. Em particular, para toda chave a, qualquer mensagem-cifrada $C < 2^{-100}$ estará nesse intervalo. Assim, podemos recuperar a simplesmente escolhendo uma mensagem-cifrada $C < 2^{-100}$ e solicitando a mensagem-plana decriptada p. Então, $a^{75} = C/p$.

Ataque known-plaintext. É possível ver que cada possibilidade dos 75 bits de escolha leva a uma imagem nas mensagens-cifradas onde existe uma correlação linear entre as mensagens-planas e as mensagens-cifradas, $C = c_r p + d_r$, onde c_r e d_r dependem dos bits de escolha r_i e da chave a. Os valores de c_r e d_r são:

$$c_r = \prod_{i=1}^{75}(a - e_i)$$

$$d_r = \sum_{i=1}^{75} r_i \prod_{j=1}^{i-1}(a - e_i).$$

Podemos ver que o valor de c_r depende apenas da quantidade n_0 de bits zero da seqüência e, e não da seqüência exata. Portanto, para um dado a, existem apenas 76 possíveis valores para c_r, que são $a^{n_0}(a-1)^{75-n_0}, n_0 \in \{0, ..., 75\}$. Os 38 valores pares de n_0 levam a valores negativos para c_r, enquanto os 38 valores ímpares de n_0 levam a valores positivos para c_r.

Dados 2^{38} mensagens-planas e seus correspondentes cifrados. Existe uma alta probabilidade de bits aleatórios. Para esse par, a diferença entre as mensagens cifradas deverá ser menor que c_r (em particular, menor que 2^{-50}, já que c_r é menor que este valor). A diferença média entre mensagens cifradas é bem maior (cerca de 2^{-38}).

No ataque sugerido por Biham, procuramos por pares de textos cifrados cuja diferença seja bastante pequena e encontrar os valores de c_r com $c_r = (c_2 - c_1)/(p_2 - p_1)$ e resolver os polinômios $c_r = a_{n_0}(a-1)^{75-n_0}$ para as 38 opções de n_0 em que c_r tenha o sinal apropriado. Cada polinômio tem no máximo duas soluções no intervalo $[0.4, 0.6]$ e a solução é verificada decriptando as mensagens-cifradas e comparando com as mensagens planas conhecidas.

Análise dos Ataques O primeiro ataque (chosen-ciphertext) tornou-se possível porque o esquema de Habutsu não deixou claro como seria definida a função (f_0 ou f_1) usada na transformação G_e. Biham determinou que essa escolha seria feita por bits inseridos na mensagem-plana, o que possibilitou o ataque. O ataque, no entanto, não seria possível se a seqüência de bits de escolha fizesse parte da chave privada. O

segundo ataque, no entanto, não faz uso da escolha dessa seqüência de bits, e teria sido possível mesmo que a seqüência fizesse parte da chave privada.

1.2.4 Cifrador de Bloco de Fridrich

Descrição Geral do Método

Em [30], Jiri Fridrich mostra como adaptar mapas caóticos bidimensionais invertíveis em um toro ou quadrado para criar esquemas de criptografia de chave simétrica. O processo de desenvolvimento de um cifrador caótico de Fridrich pode ser sumarizado como se segue. Primeiro, um mapeamento caótico é generalizado através da introdução de parâmetros de controle. Então, o mapeamento é modificado de forma a poder atuar sobre imagens compostas de um conjunto de pontos (pixels). O mapeamento é, então, estendido para três dimensões para que os valores dos pixels (nível de cinza, por exemplo) sejam trocados. Um mecanismo simples de difusão é incluído.

Escolha do Mapeamento

Fridrich sugere alguns critérios para a escolha do mapeamento a ser utilizado, que deve ser simples, de forma a permitir rápidas operações de encriptação/decriptação e permitir uma parametrização que possibilite um amplo espaço de chaves. Fridrich demonstra preferência por mapas de descrição "geométrica" simples, como o "baker map", o "cat map" e o "standard map".

Generalização

Um conjunto de parâmetros é introduzido no mapa de forma a criar parte da chave de criptografia. Como exemplo, podemos tomar o "baker map". Este mapeamento é

descrito pelas seguintes equações:

$$B(x,y) = (2x, \tfrac{y}{2}), \qquad \text{se } x \in [0, \tfrac{1}{2})$$
$$B(x,y) = (2x-1, \tfrac{y}{2} + \tfrac{1}{2}), \quad \text{se } x \in [\tfrac{1}{2}, 1].$$

Geometricamente, o mapa age sobre o quadrado unitário $[0,1] \times [0,1]$ da seguinte forma. Primeiro, o quadrado é dividido em duas colunas verticais, $[0, \frac{1}{2}) \times [0,1]$ e $[\frac{1}{2}, 1] \times [0,1]$. A primeira coluna é "contraída verticalmente" e "expandida horizontalmente" de forma a ocupar o "espaço" do retângulo horizontal $[0,1) \times [0, \frac{1}{2})$. Da mesma forma, a segunda coluna passa a ocupar o "espaço" $[0,1) \times [\frac{1}{2}, 1)$.

A generalização do "baker map" consiste na divisão do quadrado unitário em k retângulos verticais $[F_{i-1}, F_i] \times [0,1)$, $i = 1, ..., k$, $F_i = p_1 + ... + p_i$ ($p_i > 0$, $F_0 = 0$) tal que $p_1 + ... + p_k = 1$. Formalmente,

$$B(x,y) = \left(\frac{1}{p_{i+1}}(x - F_i), p_{i+1}y + F_i \right) \text{ para } (x,y) \in [F_i, F_i + p_i) \times [0,1), i = 0, ..., k-1.$$

Denotam-se o "baker map" original e sua versão generalizada por $B_{(\frac{1}{2}, \frac{1}{2})}$ e $B_{(p_1, ..., p_k)}$, respectivamente.

Discretização

Consiste na modificação do mapeamento contínuo para que ele possa ser aplicado a uma imagem composta de uma quantidade finita de pontos. O domínio do mapa é modificado, de um domínio unitário $I \times I$ para o domínio $N \times N$, $N = \{0, 1, ..., n-1\}$ (n igual ao número de pontos em uma linha ou coluna). O mapeamento discretizado F leva cada "pixel" a um outro pixel de forma bijetiva, ou seja, é uma "permutação de 'pixels'". Segundo Fridrich, a discretização deve satisfazer à seguinte propriedade assintótica:

$$\lim_{n \to \infty} \max_{0 \leq i,j \leq n} \left| f\left(\frac{i}{n}, \frac{j}{n} \right) - F(i,j) \right| = 0,$$

onde f é a "versão contínua" do mapa e F é a "versão discretizada". A fórmula acima simplesmente requer que o mapa discretizado se torne cada vez mais próximo (com a diferença tendendo a zero) do mapa contínuo, à medida que o número de "pixels" aumenta.

Uniformização do Histograma

A uniformização do histograma acontece a partir de um método de extensão do mapeamento para três dimensões. Como já explicamos, a aplicação de um mapeamento bidimensional bijetivo tem o efeito de simplesmente permutar as posições dos bits da imagem. Assim, os valores de cada "pixel" (que podem, por exemplo, representar a sua cor ou nível de cinza) simplesmente "mudam de posição". No entanto, o histograma da imagem é o mesmo antes e após a permutação.

Fridrich sugere uma pequena modificação no mapeamento caótico, de forma que os novos valores de cada "pixel" irão depender do valor anterior e da posição do pixel, de forma a uniformizar o histograma. A função sugerida modifica o valor g_{ij} do "pixel" de posição (i, j) é

$$h : N \times N \times N \to N; h(i, j, g_{ij}) = g_{ij} + \overline{h}(i, j) \ (mod\ L),$$

onde $\overline{h}$ é uma função qualquer escolhida pelo construtor do criptossistema. O único requisito para $\overline{h}$ é que a função estendida para três dimensões $B_3 : N \times N \times N \to N \times N \times N; B_3(i, j, g_{ij}) = (B(i, j), h(i, j, g_{ij}))$ seja invertível, de forma que a encriptação seja possível. Fridrich apresenta exemplo em que o histograma de imagens foi altamente uniformizado após duas iterações.

Composição com mecanismo de difusão

Os mapeamentos tridimensionais construídos da forma como a descrita por Fridrich possuem a propriedade de que a modificação do nível de cinza de um pixel da imagem original irá acarretar a modificação de um único pixel na imagem encriptada. Ou seja, um pequeno "erro" não se difunde pela imagem. Essa propriedade torna o sistema vulnerável a ataques do tipo chosen-plaintext. Um espião poderia escolher imagens cuja diferença seja apenas de um pixel e encriptá-las; a partir da comparação entre as imagens resultantes, ele aprenderia qual pixel é mapeado para onde. Repetindo esse procedimento para cada pixel da imagem, ele poderia reconstruir os parâmetros do mapeamento caótico. A única coisa restante para o criptoanalista seria descobrir a função de difusão. Fridrich sugere a inclusão de uma etapa de difusão após a permutação e a mistura dos níveis de cinza através de dois possíveis métodos. (Tais métodos de difusão não são novos e recomendamos verificar o artigo para obter maiores detalhes.)

Discussão

O cifrador proposto é baseado em mapeamentos caóticos bidimensionais, os quais são utilizados para criar permutações complexas. Ao contrário da maioria dos cifradores simétricos da atualidade, que se baseiam principalmente em complexas regras de substituição, relegando o papel das permutações a um segundo plano, este cifrador é baseado em complexas regras de substituição compostas com um mecanismo de difusão relativamente simples.

1.2.5 Outras Abordagens

Construção de S-boxes com Caos

A construção de S-boxes é uma forma de utilização do caos na criptografia que parece poder apresentar bons resultados práticos. A maioria dos cifradores práticos é composta por redes de substituição-permutação, que são etapas de transposição dos símbolos da mensagem, seguida da substituição de grupos de símbolos por outros grupos, segundo alguma regra. As S-boxes são tabelas que contém essas regras de substituição e estão divididas em dois grupos: as S-boxes fixas e as S-boxes dinâmicas.

S-Boxes Fixas. Utilizando uma abordagem convencional de projeto de cifradores, Kocarev et al. sugerem [32, 38, 39] o uso de sistemas caóticos na contrução de S-boxes. São propostos dois algoritmos para isso. No primeiro [32, 39], a S-box nada mais é do que a versão discretizada de algum sistema caótico - um mapeamento bijetivo no espaço das mensagens. No segundo [38, 39], utiliza-se a iteração de um mapeamento caótico para se gerar uma seqüência embaralhada dos inteiros $1, 2, ..., 2^n$, que é usada para gerar uma S-box $n \times n$. Trabalhos recentes têm demonstrado a resistência a ataques de criptanálise linear e diferencial.

S-Boxes Dinâmicas. Em [40] observou-se a primeira sugestão explícita do uso de caos para a geração de S-boxes dinâmicas. Shujun et al. propõem um cifrador contendo dois sub-cifradores caóticos, um de stream e um de bloco. No total são utilizados $2^n + 1$ mapas caóticos lineares por partes, dos quais 2^n são usados para encriptação (ECS - Encryption Chaotic System) e um, para controle (CCS - Control Caotic System). A condição inicial e o parâmetro do CCS são a chave secreta. No sub-cifrador de stream, os 2^n ECS's são iterados para gerar sinais de mascaramento. No sub-cifrador de bloco, uma S-box pseudo-aleatória é gerada a partir das órbitas dos 2^n

ECS's. Essa S-box é usada em substituições de símbolos da "mensagem mascarada" pelo sub-cifrador de stream.

Em [41] é proposto um cifrador de bloco com idéia semelhante: o "tent map" é iterado para gerar dinamicamente S-boxes que são usadas na encriptação da mensagem.

Cifradores Caóticos Baseados em Busca

Os cifradores de Baptista [29] e de E. Alvarez [34] efetuam uma espécie de "busca" pela mensagem-plana (ou parte dela) em uma seqüência pseudo-aleatória. Pela forma especial com que foram projetadas, torna-se difícil classificá-los como cifradores de bloco ou de stream, de forma que utilizamos a expressão "cifradores baseados em busca". Para o cifrador de Baptista, a seqüência pseudo-aleatória é a própria órbita caótica, e o conjunto atrator é particionado, sendo que a cada subconjunto corresponde um símbolo no alfabeto da mensagem-plana. Já o cifrador de E. Alvarez gera uma seqüência a partir de uma órbita caótica $\{x_n\}$ com um algoritmo de threshold: se $x_n \leq \mathfrak{U}$, então a saída é 0; se não, é 1 ($\mathfrak{U}$ pode variar). O método consiste em gerar uma seqüência pseudo-aleatória de bits e tentar localizar nela a mensagem-plana.

Método de Baptista. Passaremos, agora, a discutir um método de criptografia caótica proposto por Baptista [29] e que associa cada caractere de uma mensagem plana a um subconjunto do espaço de fase, encriptando tal caractere como o número de iterações necessárias para atingir o intervalo correspondente a partir de determinada condição inicial. Veremos que o método não é eficiente e que pode ser facilmente criptoanalisado.

Em seu trabalho, Baptista [29] descreve um método que funciona da seguinte

forma. Associa-se porções (chamadas ϵ-intervalos) do atrator aos símbolos do alfabeto onde estão definidas as mensagens. Um símbolo S_i da mensagem-plana será encriptado como o número de iterações necessária para se alcançar o ϵ-intervalo correspondente àquele símbolo, a partir de determinada condição inicial X_0.

Uma vez que se alcance o ponto p pertencente ao ϵ-intervalo correspondente ao símbolo desejado, então o ponto p passará a ser a condição inicial para encriptar o próximo caractere do texto-plano.

O processo de decriptação é bastante simples: uma vez que se conhece o sistema caótico utilizado (inclusive seus parâmetros e condição inicial), então, basta aplicar tantas iterações quanto previstas no texto cifrado.

Baptista registra algumas restrições com relação às unidades C_n de texto-cifrado (C_n é a transformação de um caractere da mensagem-plana, ou seja, o número de iterações necessárias para atingir o ϵ-intervalo associado ao caractere, partindo de determinada condição inicial). C_n deve ser maior que $N_0 = 250$ e menor que 65532. Ou seja, a encriptação de um caractere necessitará de pelo menos 250 iterações, podendo serem necessárias até 65532 iterações, levando a baixas taxas de encriptação (cerca de 100 vezes menor que as taxas de algoritmos padrão).

Segurança. O método de Baptista pode ser facilmente quebrado a partir de ataques known-plaintext. O seguinte exemplo mostra a idéia. Suponha que conhecçamos os seguintes pares de mensagens-planas/textos-cifrados:

`SUCO`: 270 300 290 310

`ELA`: 285 269 333

Embora esses pares não nos forneçam detalhes exatos a respeito dos ϵ-intervalos ou dos parâmetros do sistema dinâmico utilizado, a partir deles podemos determinar

facilmente o símbolo associado a partes da órbita:

270	S
$270 + 300 = 570$	U
$270 + 300 + 290 = 860$	C
$270 + 300 + 290 + 310 = 1180$	O
285	E
$285 + 269 =$	L
$285 + 269 + 333 =$	A

Com esse pequeno "banco de dados" já é possível recuperar os textos-planos de algumas mensagens cifradas. Por exemplo, se $c = 285\ 285$, é fácil verificar que o primeiro símbolo equivale a um 'E' (285 iterações) e o segundo, a um 'U' (285+285=570 iterações) - a palavra correponde a "EU".

Método de E. Alvarez. Já mencionamos que o cifrador de E. Alvarez et al [34] gera uma seqüência pseudo-aleatória a partir de um algoritmo de threshold (possívelmente variável). O cifrador de Alvarez procura a mensagem-plana "dentro" da seqüência pseudo-aleatória gerada.

O cifrador de Alvarez é um cifrador de bloco que encripta uma mensagem-plana em uma tripla. Ao contrário de outros cifradores convencionais, o tamanho do bloco do cifrador de Alvarez é variável. Baseado em um sistema caótico d-dimensional $x_{n+1} = F(x_n, x_{n-1}, ..., x_{n-d+1})$, o procedimento de encriptação e decriptação pode ser descrito da seguinte forma.

1. Seleciona um parâmetro de controle do sistema como chave secreta e um inteiro b_{max} como o tamanho máximo do bloco de mensagem-plana.

2. Para um bloco de mensagem-plana de tamanho $b_i = b_{max}$, escolha um threshold

$\mathfrak{U}_i$ para gerar uma cadeia de bits C_i a partir de uma órbita $\{x_n\}$ (se $x_i < 0$, a saída é um bit 0; caso contrário, a saída é 1).

3. Encontra a posição na qual o bloco de mensagem-plana ocorre em C_i e armazena $(\mathfrak{U}_i, C_i, X_i)$ como o bloco de mensagem cifrada correspondente à mensagem-plana, onde X_i é o estado do sistema dinâmico na posição, $(x_i, x_{i-1}, ..., x_{i-d+1})$.

4. Se o bloco de mensagem-plana não for encontrado em C_i após um número muito grande de iterações, decrementa-se b_i e se reinicia o processo.

Os autores utilizam o "tent map" para demonstrar o cifrador. No entanto, apenas alguns meses após a apresentação do cifrador, G. Alvarez et al. [35] mostraram que o cifrador baseado neste mapeamento poderia ser facilmente quebrado com ataques "ciphertext-only", "known-plaintext", "chosen-plaintext" e "chosen-ciphertext".

Método de Frey

Em [21], D. R. Frey usa um filtro digital com precisão finita (8 bits) em conjunto com o seu filtro inverso para implementar um codificador/decodificador. O autor define as propriedades do que denomina "comportamento quasi-caótico" e mostra que o codificador possui este comportamento. Segundo Frey, o comportamento quasi-caótico é caracterizado principalmente por apresentar, para quase toda condição inicial, um ruído de amplo espectro como resposta (saída) ao sinal de entrada.

1.2.6 Considerações gerais: Requisitos para a construção de cifradores caóticos digitais seguros

Após a análise dos diversos cifradores caóticos digitais descritos nesta seção, verificamos uma série de fraquezas comuns, a partir das quais elaboramos um sumário

de requisitos gerais que devem ser atingidos por um cifrador seguro. Descrevemos a seguir estes requisitos.

Implementação

Diversas publicações sobre criptossistemas baseados em caos contém apenas descrição de conceitos básicos, negligenciando aspectos práticos a respeito da implementação destes criptossistemas. Para que o criptossistema possa ser melhor recebido pela comunidade científica, é necessário que seja feita uma descrição da sua implementação, e se possível, com avaliações de custo e velocidade.

Chave

A chave é um dos aspectos mais importantes de um criptossitema. No entanto, observou-se trabalhos onde nem mesmo era usada uma chave (por exemplo, [42]), levando a esquemas que nada mais eram do que "codificadores". Um criptossistema não pode existir sem suas chaves estejam definidas. Além disso, o espaço de chaves deve estar claramente caracterizado, de forma a evitar regiões onde haja perda das propriedades caóticas do sistema dinâmico utilizado. O algoritmo ou processo de geração de chaves válidas deve ser especificado.

Segurança

Este é a principal preocupação para um criptossistema. Todo novo criptossistema deve ser avaliado em termos de sua segurança. Essa avaliação de segurança deve verificar a suscetibilidade a ataques: varios criptossistemas foram quebrados por ataques relativamente simples. Deve-se, também, verificar a resistência aos ataques "padrão" de criptanálise linear e diferencial. Para certas aplicações existem ataques específicos

(por exemplo, na encriptação de imagens, onde os pixels próximos costumam estar altamente relacionados) que também devem testar o criptossistema.

O criptossistema deve, também, ser resistente a ataques de força-bruta, em que se faz uma busca em todas as possíveis chaves. A eficiência de um ataque de força bruta depende do tamanho do espaço de chaves e do poder computacional disponível. Para as velocidades computacionais atuais, é um consenso que o espaço de chaves deve ser maior que 2^{100}. Alguns criptossistemas caóticos possuem um espaço de chaves bem menor que isso, e um simples "aumento de resolução" (uma discretização utilizando mais pontos), embora aumente o espaço de chaves, faz com que as chaves próximas possam tornar-se equivalentes, de forma que o problema é menos simples do que parece, merecendo um estudo cuidadoso.

No caso de cifradores que funcionem como cifradores de stream, recomenda-se um estudo de segurança que inclua testes estatísticos de aleatoriedade e verificação do tamanho do período mínimo.

Conclusão

Os requisitos descritos nesta seção não garantem a construção de um criptossistema forte. Ainda assim, ao seguir as recomendações anteriores, o pesquisador de cifradores caóticos elimina a possibilidade de incorrer em falhas comuns para este tipo de cifrador; além disso, será capaz de produzir trabalhos muito mais claros e cuja aplicabilidade poderá ser mais facilmente verificada pela comunidade científica e tecnológica.

Chapter 2

Propriedades Dinâmicas de Criptossistemas

A partir do final da década de 80 viu-se surgir um grande interesse no estudo de aplicações de sistemas caóticos para a proteção e segurança de dados. O caos tem aplicações potenciais em diversas áreas da comunicação, tais como compressão, modulação e criptografia. Os trabalhos de Matthews [11] e de Pecora e Carrol [14] abriram caminho para uma série de trabalhos sobre aplicações do caos à criptografia. Apesar da enorme quantidade de trabalhos publicada, o impacto da criptografia caótica no campo da criptografia tradicional foi muito pequeno, e apenas recentemente tem sido mais relevante.

Até o momento, a ampla maioria dos trabalhos na área de criptografia caótica se limitou à construção *ad hoc* de esquemas de criptografia. Com isso perde-se a oportunidade de se estudar as interessantes questões que surgem quando se tenta relacionar o caos e a criptografia, duas disciplinas com características relacionadas, mas que se mostram, algumas vezes, incompatíveis, devidos a seus diferentes domínios de definição. Ao mesmo tempo, eses trabalhos deram origem a esquemas muito restritos de criptografia (ao invés de métodos gerais) e que grande parte das vezes se

mostraram lentos e inseguros.

Nesta seção apresentaremos as principais ferramentas matemáticas para o estudo da criptografia, com destaque para a Teoria da Informação e seu conceito de entropia, que encontra extensão na Teoria Ergódica, esta sim, bastante relacionada com Sistemas Dinâmicos.

2.1 Teoria da Informação

A teoria da informação foi desenvolvida no final da década de 40 e tem como conceito fundamental a idéia de "entropia". Seja X uma variável aleatória que toma valores em um conjunto finito $(x_1, ..., x_n)$ com probabilidade $P(X = x_i) = p_i, 0 \leq p_i \leq 1, \sum p_i = 1$. A entropia de X é uma medida matemática da quantidade de informação fornecida por uma observação de X. De forma equivalente, a entropia é a incerteza, antes da observação de X, sobre a saída. A entropia é um conceito útil para aproximar o número médio de bits necessários para codificar os elementos de X.

Define-se a entropia ou incerteza de X como

$$H(X) = -\sum_i p_i \log p_i = \sum_i p_i \log p_i^{-1},$$

onde entende-se que a parcela valerá zero no caso em que $p_i = 0$. Embora a fórmula pareça, a primeira vista, pouco intuitiva, pode-se, com um pouco de raciocínio, entender como ela se relaciona com a quantidade de informação de um conjunto.

2.1.1 Discussão Intuitiva

Imagine que uma pessoa (à qual chamaremos A) entrega a outra (chamada B) um envelope fechado contendo uma mensagem. B quer saber o conteúdo da mensagem, no entanto, não pode abrir o envelope. Em vez disso, B deverá fazer perguntas a A

sobre o conteúdo da mensagem, as quais A poderá responder com um "sim" ou um "não" (ou qualquer outro par de respostas). Pergunta-se: qual o número mínimo de questões que, na média, será necessário fazer de forma a se descobrir o conteúdo da mensagem?

Embora o "jogo" descrito acima possa parecer sem sentido e não ter conexão com problemas reais, as questões levantadas por esta simulação têm muito a ver com várias aplicações práticas. E possuem particular interesse para esta dissertação, pois ao analisarmos um criptossistema, estamos estudando a incerteza a respeito da mensagem cifrada (o envelope fechado) e, principalmente, como essa incerteza varia à medida que vamos acumulando informações sobre o criptossistema.

Voltemos à questão das cartas. Suponha que haja apenas uma quantidade finita de mensagens possíveis. Digamos que essas mensagens sejam "*Sim.*", "*Não.*", "*Que horas são?*" e "*Oito e meia.*". (Uma outra possibilidade seria considerar todas as mensagens possíveis com um comprimento finito n.) Não é difícil encontrar um algoritmo que nos permita descobrir o conteúdo da mensagem com um mínimo de perguntas. Basta tomar todas as mensagens possíveis e agrupá-las em dois conjuntos, M_1 e M_2, cada um deles com metade do total das mensagens possíveis. Então, faz-se a pergunta: "A mensagem está em M_1?". Se estiver, reiniciamos o processo, desta vez dividindo os elementos de M_1 em dois novos conjuntos. Se não, fazemos isso com os elementos de M_2, até que o conjunto resultante tenha apenas um elemento. (Observe que a cada pergunta respondida, reduzimos a incerteza a respeito da mensagem, até à última pergunta, quando a incerteza torna-se nula.) É fácil perceber que o número de respostas necessárias é $\log_2(n)$, onde n é o número de mensagens possíveis.

Uma pequena variação sobre a simulação acima é o caso em que sabemos, *a priori*,

que certas mensagens são mais freqüentes. É natural perguntar por estas mensagens primeiro, e desta vez, dividir o conjunto das mensagens possíveis em dois conjuntos com igual probabilidade de ocorrência. Com um pouco de álgebra, pode-se mostrar que o número médio de perguntas necessárias é exatamente a entropia do conjunto, ou seja, $H(X) = -\sum_i p_i \log p_i = \sum_i p_i \log p_i^{-1}$ (onde entende-se que a parcela valerá zero no caso em que $p_i = 0$). São propriedades da entropia:

1. $0 \leq H(X) \leq \log n$

2. $H(X) = 0$ se e somente se $p_i = 0$ para todos os i exceto para um deles, para o qual $p_i = 1$ (neste caso não haverá incerteza alguma sobre a saída).

3. $H(X) = \log n$ se e somente se $p_i = 1/n$ para todo i (todas as saídas são igualmente prováveis).

Entropia conjunta, Entropia Condicional

O caminho natural, agora, é perguntar: se tenho dois envelopes, quantas perguntas devo fazer para saber o conteúdo deles? É claro (e intuitivo) que o valor máximo será $H(X) + H(Y)$, onde X e Y são as variáveis aleatórias correspondentes às probabilidades das duas mensagens. No entanto, certas combinações de mensagens são mais prováveis (ou, pelo menos, podem ser) que outras. A chamada *entropia conjunta* de X e Y, $H(X,Y)$, nos fornece a distribuição de pares de mensagens, e é dada pela fórmula

$$H(X,Y) = -\sum_{x,y} P(X = x, Y = y) \log(P(X = x, Y = y)).$$

Voltando ao nosso exemplo, o conteúdo de uma das mensagens pode ajudar a reduzir a incerteza do conteúdo da outra. Se soubermos que uma das mensagens é

Que horas são?, então será bem provável que a outra mensagem seja *Oito e meia*. A *entropia condicional* $H(X|Y)$ nos diz quantas perguntas são necessárias para se descobrir X uma vez que conhecemos Y, pode-se verificar, $H(X|Y) = H(X,Y) - H(X)$. A quantidade $H(X|Y)$ mede a quantidade de incerteza em relação a X dado que Y foi observado. São propriedades da entropia condicional:

1. $H(X,Y) \geq 0$
2. $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
3. $H(X|Y) \leq H(X)$, valendo a igualdade se e somente se X e Y são independentes.

Informação Mútua

Por fim, chegamos ao conceito de informação mútua, que é o quanto aprendemos sobre X por conhecer Y, ou ainda, o número de perguntas que deixarão de ser necessário fazer. A informação mútua ou transinformação de variáveis aleatórias X e Y é dada por $I(X;Y) = H(X) - H(X|Y)$.

Propriedades da transinformação:

1. $I(X;Y)$ pode ser pensado como a quantidade de informação que Y revela a respeito de X.
2. $I(X;Y) \geq 0$, valendo a igualdade se X e Y são independentes.
3. $I(X;Y) = I(Y;X)$.

2.1.2 Teoria da Informação e Criptografia

A teoria da informação permite quantificar a incerteza a respeito de uma variável aleatória. Do ponto de vista do criptanalista, a chave de criptografia utilizada para

uma comunicação e a mensagem-plana correspondente a uma determinada mensagem-cifrada são variáveis aleatórias, e o seu objetivo é, ao obter dados sobre a função de criptografia utilizada, reduzir a incerteza dessas variáveis aleatórias.

Informação Acessível

A publicação do trabalho de Shannon em 1949 originou a era da criptografia científica de chave secreta. Shannon forneceu uma teoria de sistemas secretos quase tão compreensiva quanto a teoria da comunicação que ele houvera estabelecido no ano anterior. No entanto, o artigo de 1949 não originou uma explosão tão grande de pesquisas em criptografia quanto o artigo de 1948 havia originado, na área de Teoria da Informação. A verdadeira explosão ocorreu com a publicação em 1976 do artigo "New Directions in Cryptography" [4], de Diffie e Hellman, onde os autores mostraram como seria possível a comunicação segura sem a transferência de uma chave secreta entre o transmissor e o receptor, estabelecendo a era da criptografia de chave pública. Eles também sugeriram o uso da teoria da complexidade como base para futuras pesquisas em criptografia

Como já explicamos, informação é a quantidade de imprevisibilidade em uma distribuição de probabilidade e é medido em termos de sua entropia. Em um sentido fundamental, o conceito de informação proposto por Shannon capta a situação de potência computacional ilimitada. No entanto, o custo computacional pode ter papel central em criptografia e, portanto, a teoria clássica da informação não fornece uma base completa para a análise de algoritmos criptográficos. Esta incompletude ficou ainda mais visível após as sugestões de Diffie e Hellman sobre as "trapdoor functions". De fato, pode ser o caso de o texto cifrado conter todas as informações sobre o texto plano e, no entanto, essa informação estar inacessível e não poder ser eficientemente

computada. Dessa forma, torna-se importante não tanto definir "informação", mas sim, "informação acessível". Em 1982, Yao mostrou que este conceito de "informação acessível" poderia ser alcançado através da combinação das teorias da Informação e da Complexidade. E esse conceito pode ser usado para discutir a segurança de criptossistemas convencionais, geradores de números pseudo-aleatórios e "trapdoors functions".

A segurança é a questão central da criptografia. Como já mencionamos, existem duas formas de segurança criptográfica. A segurança de um criptossistema pode estar baseada na inviabilidade computacional de que ele seja quebrado (segurança computacional) ou na impossibilidade de quebrá-lo mesmo usando recursos computacionais infinitos (segurança teórica da informação ou segurança incondicional). Hoje, a segurança da maioria dos criptossistemas está baseada em equivalências com uma classe de problema que, embora não provado, assume-se de difícil solução algorítmica.

Em contraste, os sistemas com segurança teórica da informação baseiam-se em em aspectos probabilísticos. No entanto, mesmo os sistemas computacionalmente seguros utilizam recursos probabilísticos, pelo menos quando se faz hipóteses sobre a criação de chaves aleatórias. A segurança teórica da informação é mais forte que a segurança computacional; no entanto, é, geralmente, bem menos prática (Shannon prova que a segurança perfeita necessita de uma chave de pelo menos o mesmo tamanho do texto a ser cifrado). Apesar de modernamente as análises de segurança de criptossistemas basearem-se em teoria da complexidade, a abordagem utilizada neste capítulo será principalmente baseada nas idéias de segurança teórica.

2.1.3 Teoria da Informação e Caos

A teoria do caos desperta a atenção pelo fato de um sistema de baixa dimensão poder exibir um comportamento complexo e imprevisível. Considere um sistema dinâmico definido pela iteração da função $F : X \to X, X \subset \mathbb{R}$. A seqüência dos pontos $(x, F(x), F^2(x), ...)$ é chamada trajetória ou órbita de x. Assumimos que F possui um atrator caótico. Isto implica que as trajetórias de dois pontos distintos, x e $\tilde{x}$, eventualmente irão se tornar completamente não-relacionadas.

A evolução de um sistema determinístico está completamente definida pelo campo F de vetores e pela condição inicial x. No entanto, determinar completamente a condição inicial exige uma medida com precisão infinita e uma quantidade infinita de informação. Como essa condição não é prática, faz-se uma medida finita. Medir (de forma finita) uma condição inicial equivale a particionar o espaço em um número finito de regiões, associando símbolos a cada região, e obtendo, em certos casos, uma dinâmica macroscópica que é chamada de dinâmica simbólica.

Se o sistema é caótico, então estados iniciais correspondendo à mesma região irão dar origem a observações diferentes em algum momento futuro. Enquanto o fluxo do sistema dinâmico contínuo é determinístico, o movimento no espaço de estados é probabilístico - baseado nos estados anteriores pode-se especificar apenas probabilisticamente a trajetória futura.

Do ponto de vista de nosso sistema de medida, se o sistema dinâmico evolui de forma "imprevisível", então o sistema é chamado de caótico. Enquanto o sistema é determinístico no espaço contínuo (microscópico), ele se torna probabilístico no espaço "particionado", onde a trajetória é uma seqüência de símbolos - as partições do estado. Com base nos estados anteriores, podemos determinar o próximo estado

apenas de forma probabilística, e a cada iteração, obtemos mais informações para determinar (ainda que probabilisticamente) o próximo estado.

2.1.4 Aplicando Teoria da Informação a Criptossistemas Práticos

Uma vez munidos das ferramentas da Teoria da Informação, podemos investigar de forma mais precisa propriedades dos criptossistemas.

Notação para definição de criptossistemas

Neste capítulo trataremos principalmente de criptossistemas de bloco, devido à maior facilidade de conectá-los com iterações de sistemas dinâmicos. Um criptossistema de bloco $S = (M, K, \{T_k\})$ é definido por um espaço de mensagens M e um conjunto de transformações $T_k : M \to M$ bijetivas e indexadas por $k \in K$, onde K é chamado "espaço das chaves".

As transformações T_k podem ser descritas como permutações no espaço M das mensagens de N bits ($\#M = 2^N$). Assim, uma transformação descrita como $T = (m_{i_1}, m_{i_2}, ..., m_{i_{2^N}})$ será a transformação que leva m_1 a m_{i_1}, m_2 a m_{i_2},..., e m_{2^N} a $m_{i_{2^N}}$. Além disso, será conveniente definir conjuntos de transformações como, por exemplo

$$\{T_k\}_{k|T_k(m_3)=m_{i_3},T_k(m_4)=m_{i_4},T_k(m_{i_{2^N-2}})=m_{i_{2^N-2}}}$$

Pela nossa notação, o conjunto acima, por exemplo, é o conjunto das transformações que levam m_3 a m_{i_3}, m_4 a m_{i_4},..., e m_{2^N-2} a $m_{i_{2^N-2}}$, precisamente composto por $(2^N - 3)!$ transformações.

Um criptossistema em particular será bastante mencionado e nos referiremos a ele por $\breve{S}$: é o criptossistema cujas transformações de encriptação são todas as possíveis bijeções no espaço das mensagens, ou seja, pela notação anteriormente descrita, $\{T_k\}_k$.

$\breve{S}$ é definido da seguinte forma:

$$M = \{m_1, m_2, ..., m_N\}$$
$$K = \{\text{conjunto das permutações de}(1, 2, ..., N)\}$$
$$T_{k,k\in K} : M \to M, T_k(m_j) = m_{i_j}$$

O criptossistema $\breve{S}$

Mostraremos que $\breve{S}$ é o mais seguro criptossistema possível baseado em cifras de blocos, que caracterizaremos como de "segurança maximal". (Consideramos, aqui, o caso em que a probabilidade "a priori" de todas as mensagens é igual. A extensão para o caso geral é simples.)

Claramente o nosso "criptossistema de segurança maximal" é o mais forte possível. Por sua definição, a incerteza a respeito de cada mensagem-cifrada é máxima, ou seja, o logaritmo do tamanho do espaço das mensagens. Após o criptoanalista obter alguns pares mensagem-plana/mensagem-cifrada, a incerteza das mensagens cifradas restantes irá diminuir, pois como a função de encriptação é bijetiva, as mensagens restantes não poderão corresponder a qualquer das mensagens-planas daqueles "pares conhecidos". Ainda assim, considerando apenas as mensagens-planas restantes (após a eliminação das i pertencentes a algum "par conhecido") a incerteza de cada mensagem cifrada é máxima, ou seja, $\log(n - i)$. É possível, também, verificar que $\breve{S}$ oferece segurança perfeita.

Como já explicamos, em um criptossistema baseado em blocos, cada chave k determina uma bijeção de M em M, ou seja, uma espécie de tabela que contém uma "regra de substituição" para cada mensagem em M. Um criptossistema contém um conjunto de "tabelas" ("regras de substituição") K. No caso do criptossistema

baseado em permutações aleatórias acima, como o K contém todas as tabelas de substituição possíveis, conhecer a regra de substituição de uma determinada mensagem não irá fornecer informação nenhuma a respeito das regras de substituição de outras mensagens (exceto que, pelo fato de T_k ser bijetiva, as outras mensagens não podem ser mapeadas para o mesmo texto-cifrado).

Evidentemente o criptossistema $\breve{S}$ é extremamente forte. No entanto, é de utilização bastante complicada, já que a chave é muito grande. De fato, se estivermos trabalhando com o espaço M das mensagens de n bits, teremos que $card(M) = 2^n$ e, portanto, existirão $2^n!$ mapeamentos bijetivos em M. De acordo com a aproximação de Stirling, temos que

$$\ln(N!) \approx N\ln(N) - N$$

$$\log_2(N!) \approx N(\log_2(N) - \log_2(e)).$$

Assim, cada chave terá tamanho

$$\log_2(2^n!) \approx 2^n(n - \log_2(e)).$$

Para dar uma idéia, se estivermos trabalhando no espaço das mensagens de 64 bits, a chave terá tamanho $1,154 \times 10^{21}$ bits. Além disso, a computação dessa encriptação será lenta, já que esta chave deverá ser inteiramente lida e deverá ser identificada a substituição correspondente.

O objetivo de qualquer criptossistema prático é reduzir o número de substituições possíveis de forma a tornar o espaço das chaves mais facilmente manipulável (representável por um número razoavelmente pequeno de bits) e as funções de encriptação mais rápidas. Um criptossistema como o "Blowfish" [23] encripta blocos de 64 bits com chaves de comprimento até 448. Assim, o objetivo de um criptossistema é obter

um subconjunto de todas as transformações bijetivas possíveis no espaço das mensagens que possua determinadas propriedades semelhantes ao criptossistema baseado em permutações aleatórias descrito nesta seção, ou seja, manter uma elevada incerteza inicial (o máximo possível) a respeito de toda mensagem cifrada e, mesmo após a obtenção de um conjunto de pares de mensagem-plana/mensagem-cifrada, mantê-la o mais elevada possível. E essa propriedade, claro, deve valer para todas as chaves (inexistência de "chaves fracas"). Procuraremos, aqui, identificar essas propriedades.

Incerteza Inicial e Redução de Incerteza

Dada C uma mensagem-cifrada por uma chave desconhecida (ao criptoanalista), existe um conjunto de mensagens-planas possivelmente correspondentes a C. A mensagem-plana correspondente a uma determinada mensagem-cifrada pode ser vista como uma variável aleatória, a qual determina uma "incerteza" para cada mensagem-cifrada. Um criptoanalista que começa a analisar mensagens criptografadas com uma chave desconhecida possui um determinado grau de incerteza associado a cada mensagen-cifrada, a "incerteza inicial". A medida que ele obtém informações a respeito do criptossistema (em nossos estudos, consideraremos principalmente a obtenção de pares de mensagens-planas/mensagens-cifradas), as incertezas tendem a diminuir. Vejamos alguns exemplos de cálculo da "incerteza inicial" e de como o conhecimento de "parte da função T_k" - ou seja, a obtenção de alguns pares mensagem-plana/mensagem-cifrada - irá fornecer ou não informação sobre o "resto da função T_k" dependendo das possíveis funções a serem utilizadas. (Cabem, aqui, duas observações. A primeira é que apesar de estarmos usando o índice k, o criptoanalista não conhece esta chave. A segunda é que quando dizemos que o criptoanalista conhece "parte de T_k", isto significa que ele conhece os valores $T_k^{-1}(\tilde{c})$ para todo $\tilde{c}$ de

um subconjunto $\tilde{C}$ de C. O objetivo do criptoanalista é saber $T_k^{-1}(\breve{c})$ para outros $\breve{c} \in C \setminus \breve{C}$.) Os exemplos a seguir ilustrarão as idéias apresentadas.

Exemplo 1) Suponha que $M = \{m_1, m_2, ..., m_8\}$. Existem 8! bijeções $T_k : M \to M$. Considere um criptossistema com a seguinte propriedade: para cada coleção de 3 pares ordenados da forma $\{(m_1, m_{\alpha_1}), (m_2, m_{\alpha_2}), (m_3, m_{\alpha_3})\}$, $\alpha_1, \alpha_2, \alpha_3 \in \{1, 2, ..., 8\}$ (ao todo são $C_8^3 = 56$) e distintos dois a dois, existe somente uma transformação T_k tal que $T_k(m_1) = m_{\alpha_1}$, $T_k(m_2) = m_{\alpha_2}$ e $T_k(m_3) = m_{\alpha_3}$. Teremos, então, um criptossistema com blocos de tamanho 8, e com 56 chaves ou possíveis T_k (uma quantidade não tão pequena, considerando o tamanho do bloco). No entanto, qualquer que seja a chave utilizada, o criptoanalista poderá quebrá-la com um ataque known-plaintext se descobrir os valores de $T_k(m_1)$, $T_k(m_2)$ e $T_k(m_3)$. Ou seja, para qualquer chave, com apenas 3 pares mensagem-plana/mensagem-cifrada, o criptoanalista descobre T_k.

Em nosso exemplo acima, escolhemos um criptossistema particularmente fraco, onde dado um conjunto de pares mensagem-plana/mensagem-cifrada, o criptoanalista é capaz de determinar unicamente a função de encriptação utilizada. De uma forma geral, um criptossistema não será tão fraco; de todo modo a obtenção de pares mensagem-plana/mensagem-cifrada irá fornecer informações a respeito da função utilizada para encriptar as mensagens. A quantidade de informação obtida irá depender da própria função utilizada (dentro daquelas possíveis no criptossistema) e dos pares obtidos.

Exemplo 2) Seja, novamente, $M = \{m_1, m_2, ..., m_8\}$. Defina um criptossistema formado pelas seguintes transformações:

$$\begin{cases} T_0(m) = \begin{cases} m_1 \text{ se } m = m_1; \\ \tau(m) : M \setminus \{m_1\} \to M \setminus \{m_1\} \text{ se } m \neq m_1 \ (\tau \text{ é uma bijeção fixada}) \end{cases} \\ \{T_k\}_{k=1,...,\gamma}, \text{ conjunto das bijeções } T_k : M \to M \text{ tais que } T_k(m_1) \neq m_1 \end{cases}$$

(são ao todo $\gamma + 1 = 7.7! + 1 = 35281$ transformações). Observe que, neste caso, obtivemos um espaço de chaves bastante grande. No entanto, se for utilizada a transformação T_0, bastará saber que $T(m_1) = m_1$) e a transformação será descoberta. Observe que ela não seria quebrada se se conhecesse o valor de $T(m_2)$ ou se se fosse utilizada outra função de encriptação.

Um criptossistema contém um conjunto de funções de encriptação que é conhecido pelo criptoanalista. Cada uma dessas funções (no caso das cifras de bloco, que estamos estudando) é uma bijeção no espaço das mensagens. Cada função de encriptação é um conjunto de $\#M$ pares $(m, T_k(m))$. O objetivo do criptoanalista é conhecer completamente a função de encriptação ou, de forma equivalente, conhecer todos os pares $(m, T_k(m))$. A cada par obtido pelo criptoanalista , podem reduzir-se as transformações possivelmente utilizadas: se o criptoanalista obtém um par (p, c), ele sabe que todas as transfomações em que $T_{\tilde{k}}(p) \neq c$ estão fora da lista de funções "candidatas". Quanto mais pares o criptoanalista obtiver, menor será o universo das funções "candidatas" e menor será a incerteza a respeito da função de encriptação utilizada.

Exemplo 3) Sejam $M = \{m_1, m_2, ..., m_8\}$ e T formado pelas transformações com as seguintes chaves:

$T_k(m_i) = m_{i_j}$, onde $k = \{j_1, ..., j_8\}$ é uma permutação de $\{1, 2, ..., 8\}$.

$K = A \cup B$, onde A são as permutações da forma $(2, 1, x_1, x_2, ..., x_6)$ e A são as permutações da forma $(x_1, 1, 2, x_2, ..., x_6)$. ($(x_1, x_2, ..., x_6)$ são as possíveis permutações de (3,4,...,8).)

Este criptossistema terá um número bastante grande de possíveis funções de encriptação (2.6!=1440). Além disso, conhecer um par mensagem-plana/mensagem-cifrada não irá reduzir muito a incerteza sobre a transformação utilizada. Ainda assim, é fácil perceber a fraqueza do criptossistema, uma vez que se o criptoanalista detectar uma mensagem cifrada m_1, ele saberá que a mensagem-plana correspondente é m_2. Além disso, se ele detectar uma mensagem cifrada m_2, ele saberá que a mensagem-plana correspondente é m_1 ou m_3.

Verificamos, então, que não apenas é importante verificar o quanto a obtenção de pares mensagem-plana/mensagem-cifrada irá reduzir a incerteza sobre a função de encriptação utilizada, mas também saber, para o criptossistema, qual a incerteza inicial a respeito de cada mensagem cifrada.

Exemplo 4) Uma "variação" do exemplo 3 mostrará o que queremos dizer com o fato de um par $(m, T_k(m))$ reduzir a incerteza de uma mensagem cifrada:

$$\{T_k\}_{k\in K|T_k(m_1)=m_2,T_k(m_2)=m_1,T_k(m_4)=m_8} \bigcup \{T_k\}_{k\in K|T_k(m_2)=m_1,T_k(m_3)=m_2,T_k(m_4)=m_8}$$
$$\bigcup \{T_k\}_{k\in K|T_k(m_1)=m_4,T_k(m_2)=m_3,T_k(m_4)=m_7} \bigcup \{T_k\}_{k\in K|T_k(m_2)=m_3,T_k(m_3)=m_4,T_k(m_4)=m_7}$$

Se o criptoanalista descobrir o valor de $T_k(m_4)$, as incertezas sobre $T_k^{-1}(m_1)$, $T_k^{-1}(m_2)$ e $T_k^{-1}(m_3)$ irão diminuir bastante. Digamos que $T_k(m_4) = m_8$. No caso de $T_k^{-1}(m_2)$, por exemplo, antes de conhecer o par $(m_4, T_k(m_4) = m_8)$, as possibilidades para $T_k^{-1}(m_2)$ eram:

$$m_1, m_3 : 30\%,$$
$$m_5, m_6, m_7, m_8 : 10\%.$$

Após a obtenção do "par", passaram a ser:

$$m_1, m_3 : 50\%.$$

Isso significa uma redução de incerteza de 1,6436 para 0,6936 (os valores podem ser conferidos utilizando a fórmula de entropia de Shannon). observe que os valores

máximos de entropia seriam $-\ln(\frac{1}{8}) = 2,0794$ antes da obtenção do par e $-\ln(\frac{1}{7}) = 1,9459$ (lembre-se de que a obtenção do par sempre elimina uma possibilidade para $T_k^{-1}(m)$, pois o mapeamento é bijetivo).

Chapter 3

Teoria Ergódica

3.1 Introdução

Ao se tratar de sistemas dinâmicos, é natural considerar a teoria ergódica, que parece apresentar relações íntimas com as propriedades dos bons criptossistemas, apesar dessas relações não estarem claras, ainda. De qualquer maneira, consideramos essas propriedades ergódicas neste capítulo.

3.2 Teoria da Medida e Teoria Ergódica: Conceitos e Terminologia

Nesta seção apresentaremos os principais conceitos, idéias e notações de Teoria da Medida e Teoria Ergódica que aplicaremos ao estudo e caracterização das propriedades de criptossistemas. Inicialmente apresentamos essas ferramentas em sua forma tradicional, para, em seguida, transpor algumas das definições para o domínio dos criptossistemas.

3.2.1 Medidas e Espaços de Medida

Def.: Uma coleção $\mathfrak{B}$ de subconjuntos de um conjunto X é uma *sigma-álgebra* se:

1. $B \in \mathfrak{B} \Rightarrow X \setminus B \in \mathfrak{B}$;

2. Dada uma seqüência enumerável $\{B_k\}$ de subconjuntos de X, com $B_k \in X$ para todo k, então a união $\bigcup_k B_k \in \mathfrak{B}$; e

3. $X \in \mathfrak{B}$.

Das propriedades (1) e (3) concluímos que $\emptyset \in \mathfrak{B}$, pois $\emptyset = X \setminus X$.

Além disso, dada uma seqüência enumerável $\{B_k\}$ de subconjuntos de X, com $B_k \in X$ para todo k, então a interseção $\bigcap_k B_k \in \mathfrak{B}$, pois $\bigcap_k B_k = X \setminus \bigcap_k (X \setminus B_k)$.

Por fim, a diferença de dois conjuntos B_1 e B_2 pertencentes a $\mathfrak{B}$, $B_1 \setminus B_2$, também pertencerá a $\mathfrak{B}$, pois $B_1 \setminus B_2 = B_1 \bigcap (X \setminus B_2)$.

Def.: Uma função a valores reais μ definida em uma sigma-álgebra $\mathfrak{B}$ é uma *medida* se:

1. $\mu(\emptyset) = 0$;

2. $\mu(B) \geq 0$ para todo $B \in \mathfrak{B}$; e

3. $\mu(\bigcup_k B_k) = \sum_k \mu(B_k)$, se $\{B_k\}$ é uma seqüência enumerável de conjuntos de $\mathfrak{B}$ disjuntos dois a dois ($B_i \bigcap B_j = \emptyset$ para $i \neq j$).

(Não excluímos a possibilidade de que $\mu(B) = \infty$ para algum $B \in \mathfrak{B}$.)

Def.: Se $\mathfrak{B}$ é uma sigma-álgebra de subconjuntos de X e μ é uma medida em $\mathfrak{B}$, então, a tripla $(X, \mathfrak{B}, \mu)$ é chamada de um *espaco de medida*. Os conjuntos de $\mathfrak{B}$ são ditos *conjuntos mensuráveis*.

Def.: Um espaço de medida $(X, \mathfrak{B}, \mu)$ é dito sigma-finito se existe uma seqüência $\{B_k\}$, $B_k \in \mathfrak{B}$, satisfazendo

$$X = \bigcup_{k=1}^{\infty} B_k \text{ e } \mu(B_k) < \infty, \text{ para todo } k.$$

Def.: Um espaço de medida $(X, \mathfrak{B}, \mu)$ é chamado *finito* se $\mu(X) < \infty$. Em particular, se $\mu(X) = 1$, o espaço de medida é dito *normalizado* ou *de probabilidade*.

Transformações que preservam uma medida

Def.: Sejam $(X_1, \mathfrak{B}_1, \mu_1)$ e $(X_2, \mathfrak{B}_2, \mu_2)$ espaços de probabilidade. Então:

1. Uma transformação $T : X_1 \to X_2$ é *mensurável* em relação a $(X_1, \mathfrak{B}_1, \mu_1)$ e $(X_2, \mathfrak{B}_2, \mu_2)$ se para todo $B_2 \in \mathfrak{B}_2$ temos $T^{-1}(B_2) \in \mathfrak{B}_1$. Neste caso, escrevemos $T : (X_1, \mathfrak{B}_1, \mu_1) \to (X_2, \mathfrak{B}_2, \mu_2)$ *mensurável*.

2. Uma transformação mensurável $T : (X_1, \mathfrak{B}_1, \mu_1) \to (X_2, \mathfrak{B}_2, \mu_2)$ *preserva a medida* se $\mu_1(T^{-1}(B_2)) = \mu_2(B_2)$ para todo $B_2 \in \mathfrak{B}_2$. Diremos também, neste caso, que μ é invariante por T.

3. Uma transformação mensurável $T : (X_1, \mathfrak{B}_1, \mu_1) \to (X_2, \mathfrak{B}_2, \mu_2)$ é *invertível* se T preserva a medida, é bijetiva, e T^{-1} também preserva a medida.

Observação: quando as sigma-álgebras e suas medidas estiverem claras, no contexto, escreveremos apenas $T : X_1 \to X_2$.

Ergodicidade

Def.: Seja $(X, \mathfrak{B}, \mu)$ um espaço de probabilidade. Uma transformação $T : (X, \mathfrak{B}, \mu) \to (X, \mathfrak{B}, \mu)$ que preserva a medidaé chamada *ergódica* se os únicos membros $B \in \mathfrak{B}$ com $T^{-1}(B) = B$ são tais que $\mu(B) = 0$ ou $\mu(B) = 1$.

A definição acima caracteriza transformações que não precisam ser estudadas a partir de sua redução a transformações mais simples. Se houvesse B com $T^{-1}(B) = B$ e $0 < \mu(B) < 1$, teríamos $T^{-1}(X \setminus B) = X \setminus B$ e $0 < \mu(X \setminus B) < 1$, e poderíamos estudar $T|_B$ e $T|_{X \setminus B}$ separadamente e de forma simplificada.

O seguinte teorema (que enunciaremos sem demonstração) caracteriza as transformações ergódicas.

Teo.: Seja $(X, \mathfrak{B}, \mu)$ um espaço de probabilidade e seja $T : X \to T$ uma transformação que preserva a medida. Então, T é ergódica se e somente se, para todos $B_1, B_2 \in \mathfrak{B}$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \mu(T^{-i}(B_1) \cap B_2) = \mu(B_1)\mu(B_2).$$

3.2.2 Teorema de Recorrência de Poincaré

Seja $T : (X, \mathfrak{B}, \mu) \to (X, \mathfrak{B}, \mu)$ uma transformação que preserva a medida do espaço de probabilidade $(X, \mathfrak{B}, \mu)$. Dado $B \in \mathfrak{B}$, seja B_0 o conjunto dos pontos $x \in B$ tais que $T^n(x) \in B$ para um número infinito de $n \geq 0$ (ou seja, existe alguma seqüência $(n_1, n_2, ...)$ tal que $T^{n_1}(x) \in B, T^{n_2}(x) \in B, ...)$. Então, $B_0 \in \mathfrak{B}$ e $\mu(B_0) = \mu(B)$.

Dem.:

Seja $C_n = \{x \in B | T^j(x) \notin B \text{ para todo } j \geq n\}$. É fácil ver que

$$B_0 = B \setminus \bigcup_{n=1}^{\infty} C_n.$$

Assim, para mostrar que $B_0 \in \mathfrak{B}$, basta mostrar que $C_n \in \mathfrak{B}$ para todo $n \geq 1$; e para mostrar que $\mu(B_0) = \mu(B)$, basta mostrar que $\mu(C_n) = 0$ também para todo $n \geq 1$.

Observe que

$$C_n = B \setminus \bigcup_{j\geq n} T^{-j}(B).$$

Logo, $C_n \in \mathfrak{B}$ para todo $n \geq 1$ e, assim, $B_0 \in \mathfrak{B}$.

Resta mostrar que $\mu(C_n) = 0$ para todo $n \geq 1$. Observe que

$$B = T^0(B) \subset T^0(B) \bigcup \left(\bigcup_{j\geq 1} T^{-j}(B) \right) = \bigcup_{j\geq 0} T^{-j}(B).$$

Logo,

$$C_n \subset \bigcup_{j\geq 0} T^{-j}(B) \setminus \bigcup_{j\geq n} T^{-j}(B).$$

Além disso, $\bigcup_{j\geq 0} T^{-j}(B)$ contém $\bigcup_{j\geq n} T^{-j}(B)$. Logo,

$$\mu(C_n) \leq \mu\left(\bigcup_{j\geq 0} T^{-j}(B)\right) - \mu\left(\bigcup_{j\geq n} T^{-j}(B)\right).$$

No entanto, como $\bigcup_{j\geq n} T^{-j}(B) = T^{-n}(\bigcup_{j\geq 0} T^{-j}(B))$, e μ é invariante por T, segue que

$$\mu\left(\bigcup_{j\geq n} T^{-j}(B)\right) = \mu\left(T^{-n}(\bigcup_{j\geq 0} T^{-j}(B))\right) = \mu\left(\bigcup_{j\geq 0} T^{-j}(B)\right).$$

Logo, $\mu(C_n) = 0$ e o teorema está demonstrado.

□

3.2.3 Propriedades das Medidas Invariantes

Denotaremos por $\mathfrak{M}(X)$ o conjunto das medidas de probabilidade da sigma-álgebra de Borel de X e por $\mathfrak{M}_T(X)$ o conjunto das medidas de $\mathfrak{M}(X)$ que são invariantes sob uma transformação $T : X \to X$.

Prop.: Se X é um espaço métrico compacto, então $\mathfrak{M}(X)$ é um espaço métrico compacto.

Utilizaremos uma topologia em $\mathfrak{M}(X)$ definida pela seguinte base:

$$V_{\phi,\varepsilon}(\mu) = \left\{\nu \in \mathfrak{M}(X) \mid \left|\int_X \phi d\nu - \int_X \phi d\mu\right| \leq \varepsilon\right\},$$

onde $\epsilon > 0$ e $\phi : X \to \mathbb{R}$ é contínua.

Seja $C^0(X)$ o espaço vetorial das funções contínuas $f : X \to \mathbb{R}$, com a seguinte norma:

$$\|f\|_0 = \sup_{x\in X} |f(x)|.$$

Como X é um espaço métrico compacto, então existe um subconjunto enumerável $(g_i)_{i>0}$ de $C^0(X)$, $g_i \neq 0$, que é denso na bola unitária $B \doteq \{f \in C^0(X) | \|f\|_0 \leq 1\}$. Considere em $C^0(X)$ a métrica

$$d(\mu,\nu) = \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\mu - \int_X g_j d\nu \right|.$$

É fácil ver que $d(\cdot,\cdot)$ é uma métrica:

$$d(\mu,\mu) = \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\mu - \int_X g_j d\mu \right| = \sum_{j=1}^{\infty} \frac{1}{2^j} \times 0 = 0,$$

$$d(\mu,\nu) = \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\mu - \int_X g_j d\nu \right| = \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\nu - \int_X g_j d\mu \right| = d(\nu,\mu), e$$

$$\begin{aligned} d(\mu,\nu) + d(\nu,\kappa) &= \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\mu - \int_X g_j d\nu \right| + \sum_{j=1}^{\infty} \frac{1}{2^j} \left| \int_X g_j d\nu - \int_X g_j d\kappa \right| \\ &= \sum_{j=1}^{\infty} \frac{1}{2^j} \left\{ \left| \int_X g_j d\mu - \int_X g_j d\nu \right| + \left| \int_X g_j d\nu - \int_X g_j d\kappa \right| \right\}. \\ &\leq \sum_{j=1}^{\infty} \frac{1}{2^j} \left\{ \left| \int_X g_j d\mu - \int_X g_j d\kappa \right| \right\} = d(\mu,\kappa). \end{aligned}$$

Precisaremos mostrar o seguinte lema:

Lema: Dada uma seqüência $\mu_n \in \mathfrak{M}(X)$, as seguintes propriedades são equivalentes:

1. $\lim_{n\to\infty} d(\mu_n, \mu) = 0$;
2. $\lim_{n\to\infty} \int_X g_i d\mu_n = \int_X g_i d\mu,$ para todo $i \geq 1$;
3. $\lim_{n\to\infty} \int_X g d\mu_n = \int_X g d\mu,$ para todo $g \in C^0(X)$.

Dem.:

(1) $\Rightarrow$ (2). Observe que,

$$d(\mu_n,\mu)=\sum_{j=1}^{\infty}\frac{1}{2^j}\left|\int_X g_j d\mu_n-\int_X g_j d\mu\right|$$

$$\geq \frac{1}{2^i}\left(\left|\int_X g_i d\mu_n-\int_X g_i d\mu\right|\right).$$

Logo,

$$\left|\int_X g_i d\mu_n-\int_X g_i d\mu\right|\leq 2^i d(\mu_n,\mu),$$

de onde se conclui que $\lim_{n\to\infty} d(\mu_n,\mu)=0$ implica $\lim_{n\to\infty}\int_X g_i d\mu_n=\int_X g_i d\mu$ $i\geq 1$.

(2) $\Rightarrow$ (3). O caso $g=0$ é trivial. Então, dado $g\in C^0(X)$ $(g\neq 0)$ e $\epsilon\geq 0$, escolha g_i tal que

$$\left\|g_i-\frac{g}{\|g\|}\right\|\leq\frac{\varepsilon}{3\|g\|}.$$

Seja n_0 tal que $n\geq n_0$ implica

$$\left|\int_X g_j d\mu_n-\int_X g_j d\mu\right|\leq\frac{\varepsilon}{3\|g\|}.$$

Então, usando $\mu(X)=\mu_n(X)=1$, $n\geq n_0$ implica

$$\left|\int_X g d\mu_n-\int_X g d\mu\right|\leq\|g\|\left|\int_X\left(\frac{g}{\|g\|}-g_i\right)d\mu_n\right|$$

$$+\|g\|\left|\int_X g_i d\mu_n-\int_X g_i d\mu\right|$$

$$+\|g\|\left|\int_X\left(g_i-\frac{g}{\|g\|}\right)d\mu\right|$$

$$\leq\|g\|\frac{\varepsilon}{3\|g\|}+\|g\|\frac{\varepsilon}{3\|g\|}+\|g\|\frac{\varepsilon}{3\|g\|}=\varepsilon.$$

(3) $\Rightarrow$ (1). Dado $\epsilon>0$, escolha j_0 tal que

$$\sum_{j=j_0+1}^{\infty}\frac{1}{2^j}\leq\frac{\varepsilon}{4}$$

Então,

$$d(\mu_n,\mu) \leq \sum_{j=1}^{j_0} \frac{1}{2^j} \left| \int_X g_j d\mu_n - \int_X g_j d\mu \right| + \sum_{j=j_0+1}^{\infty} \frac{1}{2^j} \left(\int_X |g_j| d\mu_n + \int_X |g_j| d\mu \right).$$

Como μ e μ_n são medidas de probabilidade em X e como $g_j \in B$ (ou seja, $\|g_j\| \geq 1$), então cada uma das integrais entre os parênteses da segunda parcela da soma acima vale no máximo 1. Assim, considerando o j_0 escolhido,

$$d(\mu_n,\mu) \leq \sum_{j=1}^{j_0} \frac{1}{2^j} \left| \int_X g_j d\mu_n - \int_X g_j d\mu \right| + 2\frac{\epsilon}{4}$$

Como a seqüência satisfaz a (3) (e, logo, a (2)), podemos encontrar n_0 tal que $n \geq n_0$ implica

$$\left| \int_X g_j d\mu_n - \int_X g_j d\mu \right| \leq \frac{\epsilon}{2}$$

para todo $j \geq 1$ (e, em particular, para $j = 1, ..., j_0$. Isto significa que para todo $n \geq n_0$ teremos

$$d(\mu_n,\mu) \leq \sum_{j=1}^{j_0} \frac{1}{2^j} \left| \int_X g_j d\mu_n - \int_X g_j d\mu \right| + \frac{\epsilon}{2} \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

□

Passemos, então, à demonstração da proposição. Provaremos que $\mathfrak{M}(X)$ é metrizável mostrando que a métrica $d(\cdot,\cdot)$ gera a topologia de $\mathfrak{M}(X)$. Seja $(\mu_n)_n$ uma seqüência tal que $d(\mu_n,\mu)$ se aproxima de 0; mostraremos que $\mu_n \to \mu$ na topologia de $\mathfrak{M}(X)$. Seja $V_{\epsilon,f}(\mu)$ uma vizinhança de μ (como definido anteriormente). Como $lim_{n\to\infty} d(\mu,\mu_n) = 0$, usando o lema anterior, sabemos que

$$\lim_{n\to\infty} \int_X f d\mu_n = \int_X f d\mu,$$

o que implica que $\mu_n \in V_{\epsilon,f}(\mu)$ para grandes valores de n. Isto prova que todo aberto de $\mathfrak{M}(X)$ é aberto na topologia dada por $d(\cdot,\cdot)$.

Analogamente, dado um aberto em relação a $d(\cdot,\cdot)$, que denotamos por $U \subset \mathfrak{M}(X)$, mostraremos que U é aberto na topologia de $\mathfrak{M}(X)$. Para isso, encontraremos, para todo $\mu \in U$, uma seqüência $(f_j)_{j=1\ldots m}$ ($f_j \in C^0(X)$) e um $\varepsilon > 0$ tal que $\cap_{j=1}^m V_{\epsilon,f_j}(\mu) \subset U$. Como $U \ni \mu$ é aberto na métrica de $d(\cdot,\cdot)$, podemos encontrar um $r > 0$ tal que $d(\mu,\nu) \leq r$ implica $\nu \in U$. Seja m tal que

$$\sum_{j=m+1}^{\infty} \frac{1}{2^j} \leq \frac{r}{4}.$$

Se tomarmos $f_j = g_j$ e $\varepsilon = r/2$, teremos que $\nu \in \cap_{j=1}^m V_{g_j,\frac{r}{2}}(\mu)$, o que implica

$$d(\nu,\mu) \leq \sum_{j=1}^{m} \frac{1}{2^j} \left| \int_X g_j d\mu - \int_X g_j d\nu \right| + \sum_{j=m+1}^{\infty} \frac{1}{2^j} \left(\int_X |g_j| d\mu + \int_X |g_j| d\nu \right).$$

$$\leq \sum_{j=1}^{m} \frac{1}{2^j} \frac{r}{2} + \sum_{j=m+1}^{\infty} \frac{1}{2^j} \cdot 2$$

$$\leq \frac{r}{2} + 2\frac{r}{4} = r$$

e, logo, $\nu \in U$.

Passaremos, agora, à prova da compacidade de $\mathfrak{M}(X)$. Como $\mathfrak{M}(X)$ é metrizável, isso equivale a provar que toda seqüência $(\mu_n)_{n\geq 1}$ em $\mathfrak{M}(X)$ tem uma subseqüência convergente. Associaremos a cada μ_n uma subseqüência $(\mu_n(j))_{j\geq 1}$ ($\mu_n : \mathbb{N} \to [-1,1]$) (verificar notação) dada por

$$\mu_n(j) = \int_X g_j d\mu_n.$$

Como $[-1,1]^{\mathbb{N}}$ munido da topologia produto é um espaço métrico compacto, então existe uma subseqüência $(\mu_{n_m})_{m\geq 1}$ tal que μ_{n_m}, $m \geq 1$, converge para todo j. Ou seja, para todo j a seqüência

$$\left(\int_X g_j d\mu_{n_m} \right)_{m\geq 1}$$

converge. Usando o mesmo raciocínio que na demonstração de (2) $\Rightarrow$ (3) do lema, podemos concluir que

$$\left(\int_X g d\mu_{n_m}\right)_{m\geq 1}$$

converge para todo $g \in C^0(X)$. Agora, considere o funcional $\phi : C^0(X) \to \mathbb{R}$ definido por

$$\phi(g) = \lim_{m\to\infty} \int_X g d\mu_{n_m}.$$

Claramente, se $g \geq 0$ então $\phi(g) \geq 0$ e $\phi(1) = 1$, pois μ_{n_m} é uma medida de probabilidade em X. Logo, ϕ é um funcional linear positivo e podemos aplicar o teorema de representação de Riesz, que nos diz que existe um $\nu \in \mathfrak{M}(X)$ tal que, para todo $g \in C^0(X)$,

$$\phi(g) = \int_X d\nu.$$

Isto significa que $\lim_{m\to\infty} \mu_{n_m} = \nu$ em $\mathfrak{M}(X)$.

□

Teo.: Se X é um espaço métrico compacto, então $\mathfrak{M}_T(X)$ é não-vazio.

Dado um mapa contínuo $T : X \to X$, definimos $T^* : \mathfrak{M}(X) \to \mathfrak{M}(X)$ por

$$(T^*\mu)(A) = \mu(T^{-1}(A))$$

para todo conjunto de Borel $A \in X$. O teorema será demonstrado se encontrarmos $\mu \in \mathfrak{M}(X)$ tal que $T^*\mu = \mu$ (ou seja, $T^*\mu(A) = \mu(T^{-1}(A)) = \mu(A)$. Tome um μ_0 em $\mathfrak{M}(X)$ e considere a seqüência $(\mu_n)_{n\geq 0}$ definida por

$$\mu_n = \frac{1}{n+1} \sum_{m=0}^{n} {T^*}^m \mu_0.$$

Como, pela proposição anterior, $\mathfrak{M}(X)$ é compacto, então podemos tomar uma subseqüência convergente $(\mu_{n_j})_{j\geq 1}$ e escrever $\mu = \lim_{j\to\infty} \mu_{n_j}$. Então,

$$T^*\mu_{n_j} = \frac{1}{n_j+1}\sum_{m=0}^{n_j} T^{*^{m+1}}\mu_0$$

$$= \frac{1}{n_j+1}\sum_{m=0}^{n_j} T^{*^m}\mu_0 - \frac{T^*}{n_j+1} + \frac{1}{n_j+1}T^{*^{n_j+1}}\mu_0.$$

Observe que os últimos dois termos convergem para zero quando j tende ao infinito. Logo

$$T^*\mu = \lim_{j\to\infty} T^*\mu_{n_j} = \lim_{j\to\infty} \frac{1}{n_j+1}\sum_{m=0}^{n_j} T^{*^m}\mu_0 = \lim_{j\to\infty}\mu_{n_j} = \mu.$$

□

3.2.4 Teorema Ergódico Maximal

Dada $f \in L^1(X)$, seja

$$E(f) = \left\{ x \mid \sup_{n\geq 0} \sum_{j=0}^{n} f(T^j(x)) > 0 \right\}.$$

Então,

$$\int_{E(f)} f d\mu \geq 0.$$

Dem.:

Seja

$$f_n(x) = \max_{m\in\{0,1,2,\ldots,n\}} \left\{ \sum_{j=0}^{m} f(T^j(x)) \right\} = \max\left\{ f(x), f(x)+f(T(x)), \sum_{j=0}^{n} f(T^j(x)) \right\}.$$

Como

$$E(f) = \bigcup_{n=0}^{\infty} \{x | f_n(x) > 0\}$$

e a união à direita é monótona ($\{x|f_n(x) > 0\} \subset \{x|f_{n+1}(x) > 0\}$), basta mostrar que

$$\int_{\{x|f_n(x)>0\}} f d\mu \geq 0$$

para todo $n \geq 0$. Observe que, por definição,

$$f_n(x) \geq \sum_{j=0}^{m} f(T^j(x)), m = 1, 2, ..., n.$$

o que implica

$$f_n(T(x)) \geq \sum_{j=0}^{n} f(T^j(T(x))) = \sum_{j=1}^{n+1} f(T^j(x)), m = 1, 2, ..., n,$$

$$f_n(T(x)) + f(x) \geq \sum_{j=0}^{n+1} f(T^j(x)), m = 1, 2, ..., n.$$

Além disso,

$$f_n(T(x)) = \max_{0\leq m\leq n} \sum_{j=0}^{m} f(T^j(x)) \leq \max_{0\leq m\leq n+1} \sum_{j=0}^{m} f(T^j(x))$$

$$= \max \left\{ f(x), \max_{0\leq m\leq n} \sum_{j=0}^{m+1} f(T^j(x)) \right\}$$

Usando as duas desigualdades anteriores, e observando que $f_n(T(x)) \geq 0$ implica $f_n(T(x)) + f(x) \geq f(x)$, obtemos

$$f_n(T(x)) \geq 0 \Rightarrow f_n(T(x)) + f(x) \geq f_n(x).$$

Observe, agora, que

$$\int_{\{f_n\geq 0\}} f d\mu = \int_{\{f_n\geq 0\}\cap\{f_n\circ T<0\}} f d\mu + \int_{\{f_n\geq 0\}\cap\{f_n\circ T\geq 0\}} f d\mu.$$

Considerando a última igualdade, segue que

$$\int_{\{f_n\geq 0\}} f d\mu \geq \int_{\{f_n\geq 0\}\cap\{f_n\circ T<0\}} f d\mu + \int_{\{f_n\geq 0\}\cap\{f_n\circ T\geq 0\}} f_n d\mu - \int_{\{f_n\geq 0\}\cap\{f_n\circ T\geq 0\}} (f_n\circ T) d\mu.$$

Mostraremos, agora, que se $f_n(x) \geq 0$ e $f_n(T(x)) < 0$, então $f_n(x) = f(x)$. Além disso (como $f_n(x) \geq 0$) $f(x) \geq 0$. É fácil ver isso pois

$$f_n(x) = \max\{f(x), f(x) + f(T(x)), \sum_{j=0}^{n} f(T^j(x))\}.$$

e

$$f_n(T(x)) = \max\{f(T(x)), f(T(x)) + f(T^2(x)), \sum_{j=1}^{n+1} f(T^j(x))\}.$$

Assim, se $f_n(T(x)) < 0$, isso significa que, para todo $m = 0, ..., n$, $\sum_{j=1}^{m+1} f(T^j(x)) = \sum_{j=0}^{m} f(T^{j+1}(x)) < 0$. Daí segue que $\sum_{j=1}^{m} f(T^j(x)) < 0$. Por outro lado, como $f_n(x) \geq 0$, existe algum m para o qual $\sum_{j=0}^{m} f(T^j(x)) \geq 0$. Logo, como (para esse m)

$$\sum_{j=1}^{m} f(T^j(x)) < 0$$

e

$$\sum_{j=0}^{m} f(T^j(x)) \geq 0$$

concluímos que $f(x) > 0$ $f(x) = f_n(x)$.

Voltando à desigualdade encontrada anteriormente,

$$\int_{\{f_n \geq 0\}} f d\mu = \int_{\{f_n \geq 0\} \cap \{f_n \circ T < 0\}} f d\mu + \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} f_n d\mu - \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} (f_n \circ T) d\mu,$$

e usando a informação de que $f_n(x) \geq 0$ e $f_n(T(x)) < 0$ implicam $f_n(x) = f(x)$ e $f(x) \geq 0$ e podemos deduzir que

$$\int_{\{f_n \geq 0\}} f d\mu = \int_{\{f_n \geq 0\} \cap \{f_n \circ T < 0\}} f_n d\mu + \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} f_n d\mu - \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} (f_n \circ T) d\mu.$$

$$\int_{\{f_n \geq 0\}} f_n d\mu - \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} (f_n \circ T) d\mu.$$

$$\int_{T^{-1}(\{f_n \geq 0\})} f_n \circ T d\mu - \int_{\{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}} (f_n \circ T) d\mu.$$

No entanto, $T^{-1}(\{f_n \geq 0\}) = \{f_n \circ T \geq 0\} \supset \{f_n \geq 0\} \cap \{f_n \circ T \geq 0\}$ e a diferença diferença acima é não-negativa. Assim,

$$\int_{\{f_n \geq 0\}} f d\mu \geq 0$$

e o teorema está demonstrado.

□

3.2.5 Teorema Ergódico de Birkhoff

Sejam $(X, \mathfrak{B}, \mu)$ um espaço de probabilidade e $T : (X, \mathfrak{B}, \mu) \to (X, \mathfrak{B}, \mu)$ uma transformação que preserva a medida. Então, se $f \in L^1(X)$, o limite

$$\lim_{n \to \infty} \frac{1}{n} \sum_{j=0}^{\infty} f(T^j(x))$$

existe em quase todo ponto $x \in X$ e função $\tilde{f}$ definida por

$$\tilde{f} = \lim_{n \to \infty} \frac{1}{n} \sum_{j=0}^{\infty} f(T^j(x))$$

satisfaz

$$\tilde{f}(T(x)) = \tilde{f}(x)$$

em quase todo ponto.

Por fim, para toda $f \in L^p(X)$, temos

$$\int_X \tilde{f} d\mu = \int_X f d\mu.$$

Dem.: Para a demonstração, precisaremos do seguinte lema, que é uma conseqüência do Teorema Ergódico Maximal

Lema: Dada $f \in L^1(X)$, defina

$$E(f) = \left\{ x \in X | \sup_{n \geq 0} \sum_{j=0}^{n} f(T^j(x)) > 0 \right\}.$$

Então, se $B \subset E(f)$ pertence a $\mathfrak{B}$ e $T^{-1}(B) = B$,

$$\int_B f d\mu \geq 0.$$

Demonstração do lema: Como $T^{-1}(B) = B$, segue que $E(1_B f) \subset B$, onde 1_B é a função característica de B. Como $B \subset (E(f))$ por hipótese, segue que $E(1_B f) = B$. Pelo Teorema Ergódico Maximal,

$$0 \leq \int_{E(1_B f)} 1_B f d\mu = \int_B 1_B f d\mu = \int_B f d\mu.$$

□

Passemos, então à demonstração do Teorema. Para $f \in L^1(X)$, defina:

$$E_\alpha^+(f) = \left\{ x \in X \mid \limsup_{n \to \infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x)) > \alpha \right\}$$

e

$$E_\alpha^-(f) = \left\{ x \in X \mid \liminf_{n \to \infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x)) < \alpha \right\}.$$

Observe que $E_\alpha^+(f) = E_0^+(f - \alpha)$ e $E_\alpha^-(f) = E_{-\alpha}^+(-f)$.

Observe, também, que

$$\int_{E_\alpha^+(f)} f d\mu = \int_{E_\alpha^+(f)} (f - \alpha) d\mu + \alpha\mu(E_\alpha^+(f)) = \int_{E_0^+(f-\alpha)} (f - \alpha) d\mu + \alpha\mu(E_\alpha^+(f)).$$

Como $T^{-1}(E_0^+(f - \alpha)) = E_0^+(f - \alpha)$ e $E_0^+(f - \alpha) \subset E(f - \alpha)$, o lema nos diz que

$$\int_{E_0^+(f-\alpha)} (f - \alpha) d\mu \geq 0.$$

Combinando a desigualdade acima com a observação anterior, obtemos

$$\int_{E_\alpha^+(f)} f d\mu \geq \alpha\mu(E_\alpha^+(f)),$$

para toda $f \in L^1(X)$ e $\alpha \in \mathbb{R}$.

Se $B \in \mathfrak{B}$ está contido em $E_\alpha^+(f)$ e satisfaz $T^{-1}(B) = B$, então, também pelo lema, podemos escrever

$$\int_B f d\mu = \int_B 1_B f d\mu = \int_{E_\alpha^+(1_B f)} 1_B f d\mu \geq \alpha\mu(E_\alpha^+(1_B f)) = \alpha\mu(B).$$

Usando a desigualdade acima e a igualdade $E_\alpha^-(f) = E_{-\alpha}^+(-f)$ (mostrada mais acima), segue que, para $f \in L^1(X)$ e $B \in (B)$ contido em $E_\beta^-(f)$ e satisfazendo $T^{-1}(B) = B$, temos

$$\int_B f d\mu \leq \beta\mu(B).$$

Usando as duas últimas desigualdades com $\alpha > \beta$ e $B = E_\alpha^+(f) \bigcap E_\beta^-(f)$, obtemos

$$\int_B f d\mu \geq \alpha\mu(E_\alpha^+(f) \cap E_\beta^-(f))$$

e

$$\int_B f d\mu \leq \beta\mu(E_\alpha^+(f) \cap E_\beta^-(f))$$

de onde obtemos (como $\alpha > \beta$)

$$\mu(E_\alpha^+(f) \cap E_\beta^-(f)) = 0.$$

Por fim, tomamos uma seqüência $(\alpha_n)_{n\geq 1}$ densa em $\mathbb{R}$ e escrevemos

$$\left\{ x \in X \mid \limsup_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x)) > \liminf_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x)) \right\} = \bigcup_{\alpha_n > \alpha_m} E_{\alpha_n}^+(f) \cap E_{\alpha_m}^-(f),$$

que tem medida zero, como já mostramos anteriormente. Assim, demonstramos que $\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{\infty} f(T^j(x))$ existe em quase todo ponto $x \in X$. □ Mostraremos, agora, que $\tilde{f}(T(x)) = \tilde{f}(x)$:

$$\tilde{f}(T(x)) = \lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(T(x))) = \lim_{n\to\infty} \left(\frac{1}{n} \sum_{j=0}^{n} f(T^j(x)) - \frac{1}{n} f(x) \right)$$

$$= \lim_{n\to\infty} \frac{n+1}{n} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x)) - \lim_{n\to\infty} \frac{1}{n} f(x)$$

$$= \lim_{n\to\infty} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x)) = \tilde{f}(x).$$

q.e.d.

Suponha, agora, que T preserva a medida e $f \in L^p(X)$, $1 \leq p < \infty$. Conforme já mostramos, o limite $\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(T^j(x))$ existe em quase todo ponto. Observe, então, que

$$|\tilde{f}(x)| \leq \lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} |f(T^j(x))|$$

em quase todo ponto. Logo,

$$|\tilde{f}(x)|^p \leq \lim_{n\to\infty} \left(\frac{1}{n} \sum_{j=0}^{n-1} |f(T^j(x))| \right)^p$$

Como $|\tilde{f}(x)|^p$ é uma função positiva, ela será integrável se a função acima definida pelo limite o for. E, pelo lema de Fatou, ela será integrável se mostrarmos que

$$\liminf_{n\to\infty} \int_X \left(\frac{1}{n} \sum_{j=0}^{n-1} |f \circ T^j| \right)^p d\mu < \infty$$

Agora,

$$\int_X \left(\frac{1}{n} \sum_{j=0}^{n-1} |f \circ T^j| \right)^p d\mu = \left\| \frac{1}{n} \sum_{j=0}^{n-1} |f \circ T^j| \right\|$$

$$\leq \left(\frac{1}{n} \sum_{j=0}^{n-1} \|f \circ T^j\|_p \right)^p$$

$$= \left(\frac{1}{n} \sum_{j=0}^{n-1} \|f\|_p \right)^p = \|f\|_p^p,$$

onde na penúltima igualdade usamos o fato de que T (e, logo, T^j) preserva a medida. Segue, então, que $|\tilde{f}|^p$ é integrável e sua integral tem valor menor que $\|f\|_p^p$. Em outras palavras, $\tilde{f} \in L^p(X)$ e $\|\tilde{f}\|_p \leq \|f\|_p$.

3.2.6 Mapas Unicamente Ergódicos

Estudaremos, aqui, o caso em que mapas contínuos de espaços métricos compactos possui exatamente uma medida invariante, ou seja, $\#\mathfrak{M}_T(X) = 1$. O seguinte teorema caracteriza mapas unicamente ergódicos em termos da média orbital de funções contínuas.

Teo.: Seja X um espaço métrico compacto e $T : X \to X$ um mapa contínuo. Então, as seguintes propriedades são equivalentes:

1. T é unicamente ergódico

2. para toda $f \in C^0(X)$ o limite $\lim_{n\to\infty} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x))$ existe para todo x e não depende de x.

3. para toda $f \in C^0(X)$ a seqüência de funções $\frac{1}{n+1} \sum_{j=0}^{n} f \circ T^j$ converge uniformemente para uma constante.

Dem.:

(1) $\Rightarrow$ (3). Suponha que (3) é falso. Então, existe $f \in C^0(X)$ tal que a seqüência $\frac{1}{n+1} \sum_{j=0}^{n} f \circ T^j$ não converge uniformemente para

$$\int_X f d\mu,$$

onde μ é o único elemento de $\mathfrak{M}_T(X)$. Então, existe um $\varepsilon > 0$, uma seqüência divergente de inteiros $(n_i)_{i\geq 1}$ e uma seqüência $(x_i)_{i\geq 1}$ de pontos de X tais que

$$\left| \frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x)) - \int_X f d\mu \right| \geq \varepsilon$$

para todo i. De acordo com o teorema de representação de Riesz, existe uma medida $\mu_{n_i} \in \mathfrak{M}(X)$ tal que

$$\int_X g d\mu_{n_i} = \frac{1}{n_i+1} \sum_{j=0}^{n_i} g(T^j(x_i)).$$

Como $\mathfrak{M}(X)$ é compacto (teorema demonstrado anteriormente), podemos assumir que a seqüência (μ_{n_i}) converge para $\nu \in \mathfrak{M}(X)$.

Agora, seja $g \in C^0(X)$. Então,

$$\int_X (g \circ T) d\nu = \lim_{n_i \to \infty} \int_X (g \circ T) d\mu_{n_i} = \lim_{n_i \to \infty} \frac{1}{n_i+1} \sum_{j=0}^{n_i} g(T^{j+1}(x_i))$$

$$= \lim_{n_i \to \infty} \int_X g d\mu_{n_i} - \lim_{n_i \to \infty} \frac{1}{n_i+1} g(x_i) + \lim_{n_i \to \infty} \sum_{j=0}^{n_i} g(T^{n_i+1}(x_i)) = \int_X g d\nu,$$

de forma que $\nu \in \mathfrak{M}_T(X)$. Por outro lado,

$$\left| \int_X f d\nu - \int_X f d\mu \right| = \lim_{n_i \to \infty} \left| \int_X f d\mu_{n_i} - \int_X f d\mu \right|$$

$$= \lim_{n_i \to \infty} \left| \frac{1}{n_i+1} \sum_{j=0}^{n_i} f(T^j(x_i)) - \int_X f d\mu \right| \geq \varepsilon,$$

de forma que $\nu \neq \mu$, contradizendo o fato de que T é unicamente ergódico.

(3) $\Rightarrow$ (2). Trivial.

(2) $\Rightarrow$ (1). Seja $\phi : C^0(X) \to \mathbb{R}$ o funcional definido por

$$\phi(f) = \lim_{n \to \infty} \frac{1}{n+1} \sum_{j=0}^{n} j(T^j(x)).$$

Então, para uma medida $\mu \in \mathfrak{M}_T(X)$, como

$$\int_X f d\mu = \int_X (f \circ T^j) d\mu$$

para todo j, obtemos

$$\int_X f d\mu = \frac{1}{n+1} \sum_{j=0}^{n} \int_X (f \circ T^j) d\mu.$$

Como a seqüência $\frac{1}{n+1} \sum_{j=0}^{n} f(T^j(x))$ é limitada por $\|f\|_0$, segue, do teorema da convergência dominada, que

$$\int_X f d\mu = \lim_{n\to\infty} \frac{1}{n+1} \sum_{j=0}^{n} \int_X (f \circ T^j) d\mu$$

$$= \int_X \lim_{n\to\infty} \left(\frac{1}{n+1} \sum_{j=0}^{n} (f \circ T^j) d\mu \right) = \int_X \phi(f) d\mu = \phi(f).$$

Logo, o único elemento de $\mathfrak{M}_T(X)$ é a medida associada ao linear funcional positivo ϕ.

□

Chapter 4

Sincronização de Caos e Aplicações à Criptografia

Neste capítulo descrevemos os conceitos relacionados aos chamados sistemas *controle-resposta* e à sincronização de sistemas caóticos, que levam a idéias e aplicações muito interessantes para a comunicação de dados.

4.1 Sincronização de Caos

4.1.1 Sistemas dependentes de um sinal externo

O estudo de sistemas que dependem de um sinal de valor variável no tempo é baseado em conceitos bastante simples. Uma forma de visualizar estes sistemas é através da seguinte expressão:

$$x^{(n)} = f(x^{(n-1)}, ..., \ddot{x}, \dot{x}, x, A(t)),$$

onde x é um vetor n-dimensional.

Um exemplo deste tipo de sistema é o de um oscilador forçado. Tal sistema pode ser descrito da forma

$$\ddot{x} - x = \sin(t).$$

No sistema acima, o sinal que determina o comportamento do sistema é $\sin(t)$. Um tópico clássico bastante estudado é o de sistemas dinâmicos controlados por sinais periódicos, como por exemplo, as equações de Duffing:

$$\ddot{x} + \delta\dot{x} - x + x^3 = \gamma\cos(\omega t),$$

onde mais uma vez uma força externa senoidal é aplicada.

Ao longo deste capítulo iremos estudar sistemas dinâmicos dependentes de um sinal externo e o interessante resultado de que, em certos casos, sistemas caóticos acoplados podem sincronizar.

Sistemas controle-resposta

Um sistema controle-resposta é formado por dois subsistemas acoplados de tal forma que o comportamento do segundo depende do comportamento do primeiro, mas este não é influenciado pelo comportamento do segundo. Nestas condições, o primeiro subsistema é chamado de sistema de controle e o segundo é chamado de sistema de resposta:

$$\begin{cases} \dot{x_1} & = Q_1(x_1, \ldots, x_q), \\ \dot{x_q} & = Q_q(x_1, \ldots, x_q), \\ \vdots & \\ \dot{x_{q+1}} & = P_1(x_1, \ldots, x_n), \\ \dot{x_n} & = P_{n-q}(x_1, ..., x_n). \end{cases}$$

Além disso, podemos dividir o subsistema de controle entre as variáveis que têm influência no subsistema de resposta e aquelas que não têm. Assim, teremos nosso

sistema inicial dividido em três subsistemas. Suponha que um sistema é decomponível dessa forma. Sejam n a dimensão do sistema e

- v o vetor m-dimensional que representa as variáveis do subsistema de controle que têm influência no subsistema de resposta,
- u o vetor k-dimensional que representa as variáveis do subsistema de controle que não têm influência no subsistema de resposta,
- w o vetor l-dimensional que representa as variáveis do subsistema de resposta.

Então $n = m + k + l$ e nosso sistema estará dividido da seguinte forma:

$$\begin{cases} \dot{u} = f(u, v), \\ \dot{v} = g(u, v), \\ \dot{w} = h(v, w). \end{cases}$$

Existem duas classificações para sistemas controle-resposta. No caso dos sistemas chamados heterogêneos, as funções f e h são diferentes. O caso em que $k = l$ e $f = h$, o controle é denominado homogêneo. De forma intuitiva, nos sistemas homogêneos, a resposta é regida pelas mesmas "regras" que o subsistema de controle indireto, levando ao conceito de sincronização entre esses subsistemas. O esquema abaixo facilitará a visualização.

$$\begin{cases} \dot{u} = f(u, v) & \text{controle indireto} \\ \dot{v} = g(u, v) & \text{controle direto} \\ \dot{w} = f(v, w) & \text{resposta direto} \end{cases}$$

A construção de um subsistema homogêneo é simples. Parte-se de um sistema dinâmico e divide-se o sistema em dois subsistemas, v e u. Então, duplica-se o

subsistema de controle indireto u, chamando-o de w e renomeando as variáveis. O sistema resultante será um sistema controle-resposta homogêneo. As formas de se gerar um sistema controle-resposta sincronizado a partir de um sistema dinâmico, e como garantir e provar a sincronização serão assuntos discutidos ao longo deste texto. De forma genérica, o que desejamos, em termos de sincronização, é que para todas as condições iniciais $u(0), v(0), w(0)$, tenhamos $(u - w)(t) \to 0$ quando $t \to \infty$.

4.1.2 Exemplo: O Sistema de Lorenz

Iremos, a seguir, apresentar um exemplo prático de aplicação dos conceitos discutidos até aqui aplicados ao sistema de Lorenz. O objetivo desta seção é fixar e exemplificar estes conceitos. O sistema de Lorenz é definido da forma a seguir:

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = -xz + rx - y, \\ \dot{z} = xy - bz. \end{cases}$$

onde os valores de σ e b geralmente são estudados como constantes valendo 10 e $\frac{8}{3}$, respectivamente, e r é um parâmetro positivo. Originalmente, o sistema de Lorenz foi concebido para modelar aspectos da convecção de fluidos no ambiente. Sabe-se que seu comportamento é caótico para determinados valores de parâmetros. Para construir um sistema controle-resposta a partir do sistema de Lorenz, definimos como subsistema de controle indireto as equações que regem a evolução de y e de z:

$$\begin{cases} \dot{y} = -xz + rx - y, \\ \dot{z} = xy - bz, \end{cases}$$

Em seguida, duplicamos as equações acima, renomeando y e z para y_2 e z_2. O

sistema final, de dimensão 5, fica como abaixo:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = -xz + rx - y \\ \dot{z} = xy - bz \\ \dot{y_2} = -xz_2 + rx - y_2 \\ \dot{z_2} = xy_2 - bz_2 \end{cases} \begin{matrix} \left.\begin{matrix} \\ \end{matrix}\right] \text{Controle Direto} \\ \left.\begin{matrix} \\ \\ \end{matrix}\right] \text{Controle Indireto} \\ \left.\begin{matrix} \\ \\ \end{matrix}\right] \text{Resposta} \end{matrix}$$

Através de simulações numéricas, pode-se observar, em certas condições, sincronização.

4.1.3 Alguns resultados sobre a sincronização do sistema estendido de Lorenz

Na seção anterior, foi apresentado um sistema de Lorenz estendido para um sistema composto de controle-resposta onde o sinal x era o sinal de controle. De acordo com a nossa notação, $u = [y, z]$ e $v = [x]$ são as variáveis do subsistema de controle e $w = [y_2, z_2]$ são as variáveis do subsistema de resposta. O sistema estendido gerado foi

$$\begin{cases} \dot{u} = (\dot{y}, \dot{z}) = (-xz + rx - y, xy - bz) = f(u, v), \\ \dot{v} = (\dot{x}) = (\sigma(y - x)) = g(u, v), \\ \dot{w} = (\dot{x_2}, \dot{z_2}) = (-xz_2 + rx - y_2, x_2y - bz_2) = h(v, w). \end{cases}$$

De forma similar, podemos obter o seguinte sistema extendido para o caso em que a variável de controle é y:

$$\begin{cases} \dot{u} = (\dot{x}, \dot{z}) = (\sigma(y - x), xy - bz) = f(u, v), \\ \dot{v} = (\dot{y}) = (-xz + rx - y) = g(u, v), \\ \dot{w} = (\dot{x_2}, \dot{z_2}) = (\sigma(y - x_2), x_2 y - bz_2) = h(v, w). \end{cases}$$

Se z é o sinal de controle:

$$\begin{cases} \dot{u} = (\dot{x}, \dot{y}) = (\sigma(y - x), -xz + rx - y) = f(u, v), \\ \dot{v} = (\dot{z}) = (xy - bz) = g(u, v) \\ \dot{w} = (\dot{x_2}, \dot{y_2}) = (\sigma(y_2 - x_2), x_2 z + r x_2 - y_2) = h(v, w) \end{cases}$$

Simulações com o sistema controlado por y sugerem que há sincronização. O mesmo não acontece com o sistema controlado por z. Porém, no caso deste último sistema, se observarmos x_2/x e y_2/y, observaremos a convergência dessas duas proporções para o mesmo valor. De certa forma, as trajetórias de (x_2, y_2) são uma cópia amplificada de (x, y).

Prova direta da sincronização do sistema

Na seção anterior, mostramos como aparentemente os sistemas estendidos de Lorenz controlados por x e por y parecem apresentar sincronização. Nesta seção, daremos provas de que a sincronização de fato acontece. As técnicas aqui empregadas não são o que existe de mais geral em sincronização de sistemas dinâmicos, mas funcionam bem para os sistemas que temos estudado até o momento.

Proposition 4.1.1. *As soluções da equação de Lorenz são limitadas para $T \geq 0$.*

Dem.: Seja $(x(t), y(t), z(t))$ solução da equação de Lorenz e

$$V(x, y, z) = \frac{1}{2}(rx^2 + \sigma y^2 + \sigma(z - 2r)^2),$$

definida para todo $x, y, z \in \mathbb{R}$. Temos que

$$\begin{aligned}
\frac{d}{dt}V(x(t), y(t), z(t)) &= rxx' + \sigma yy' + \sigma(z - 2r)z' \\
&= rx(\sigma(y - x)) + \sigma y(rx - y - xz) + \sigma(z - 2r)(xy - bz) \\
&= r\sigma xy - r\sigma x^2 + r\sigma xy - \sigma y^2 - \sigma xyz + \sigma xyz - 2r\sigma xy - b\sigma(z - 2r)z \\
&= -r\sigma x^2 - \sigma y^2 - b\sigma(z - 2r)^2 - b\sigma(z - 2r)2r \\
&\leq -r\sigma x^2 - \sigma y^2 - b\sigma(z - 2r)^2 + \frac{b\sigma}{2}(z - 2r)^2 + 2\sigma br^2 \\
&\leq -r\sigma x^2 - \sigma y^2 - \frac{b\sigma}{2}(z - 2r)^2 + 2\sigma br^2.
\end{aligned}$$

Agora, defina $\lambda = \min\{2\sigma, 2, b\}$ e $\gamma = 2\sigma br^2$. Podemos escrever, então,

$$\frac{d}{dt}V \leq -\lambda V + \gamma.$$

Usando o fator de integração $e^{-\lambda t}$, obtemos

$$V(x(t), y(t), z(t)) \leq V(x(0), y(0), z(0))e^{-\lambda t} + \frac{\gamma}{\lambda}.$$

Isso mostra que as soluções são limitadas em $t \geq 0$ e são atraídas para a elipsóide $V = \gamma/\lambda$.

Proposition 4.1.2. *O sistema homogêneo de Lorenz controlado por y sincroniza.*

Dem: Se y é o sinal de controle, podemos particionar o sistema da seguinte forma:

$$\begin{cases}
x' = \sigma(y - x), \\
y' = -xz + rx - y, \\
z' = xy - bz, \\
x_2' = \sigma(y - x_2), \\
z_2' = x_2 y - bz_2.
\end{cases}$$

Estamos interessados na magnitude de $e_1 = x - x_2'$ e $e_3 = z - z_2'$ como funções do tempo, e esperamos que estas quantidades vão para zero quando t tende a infinito.

Observe que

$$e_1' = -\sigma e_1,$$

$$e_3' = e_1 y - b e_3.$$

Da primeira das equações acima, verificamos que $e_1(t) = C_1 e^{-\sigma t}$, onde C_1 é uma constante relacionada às condições iniciais. É evidente que, para $\sigma > 0$, $e_1 \to 0$ quando $t \to \infty$.

Na segunda equação, como as soluções da equação de Lorenz são limitadas, em particular, $y(t)$ é limitado. Usando o fator de integração e^{bt}, obtemos

$$e_3(t) = C_3 e^{-bt} + e^{-bt} \int_0^t e^{bs} e_1(s) y(s) ds.$$

Temos, fazendo $Y = \sup_{t \geq 0} y(t)$, que

$$\begin{aligned} |e^{-bt} \int_0^t e^{bs} e_1(s) y(s) ds| &\leq e^{-bt} \int_0^t e^{bs} C_1 e^{-\sigma s}(s) Y ds \\ &\leq \begin{cases} C_1 Y e^{-bt} \left(\dfrac{e^{(b-\sigma)t} - 1}{b - \sigma} \right), \text{ se } b \neq \sigma \\ C_1 Y e^{-bt} t, \text{ se } b = \sigma \end{cases} \\ &\leq \begin{cases} C_1 Y \dfrac{e^{-\sigma t}}{b - \sigma} \to 0 \text{ quando } t \to \infty, \text{ se } b \neq \sigma \\ C_1 Y e^{-bt} t \to 0 \text{ quando } t \to \infty, \text{ se } b = \sigma \end{cases} \end{aligned}$$

Assim, $e_1 \to 0$ e $e_3 \to 0$ quando $t \to \infty$. Em particular, $x \to x_1$ e $z \to z_1$; então, para y como sinal de controle, ocorre sincronização.

Proposition 4.1.3. *O sistema homogêneo de Lorenz controlado por x sincroniza.*

Prova: Se x é o sinal de controle, podemos particionar o sistema da seguinte forma:

$$\begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = -xz + rx - y, \\ \dot{z} = xy - bz, \\ \dot{y_2} = -xz_2 + rx - y_2, \\ \dot{z_2} = xy_2 - bz_2. \end{cases}$$

.

Definimos, agora, $e_2 = y - y_2$ e $e_3 = z - z_2$. Observe que

$$e_2' = -xe_3 - e_2,$$

$$e_3' = xe_2 - be_3.$$

Multiplicando a primeira equação por e_2 e adicionando à segunda multiplicada por e_3, obtemos

$$e_2e_2' + e_3e_3' = -(e_2^2 + be_3^2).$$

O lado esquerdo é metade da derivada da soma dos quadrados de e_2 e e_3. Assim, obtemos:

$$\frac{d}{dt}(e_2^2 + e_3^2) = -2(e_2^2 + be_3^2).$$

Temos que $(e_2^2 + e_3^2)(t) \geq 0, \forall t$, e como $b > 0$, pela equação acima sua derivada é negativa para todo $e_2, e_3 \neq 0$ e é nula somente para $e_2 = e_3 = 0$. Logo, $(e_2^2+e_3^2)(t) \to 0$ quando $t \to \infty$. Ou seja, $e_2 \to 0$ e $e_3 \to 0$ e temos a sincronização.

Podemos ser mais precisos considerando $\min\{1, b\}$ e obtendo o decaimento exponencial $e_2^2(t) + e_3^2(t) \leq (e_2(0)^2 + e_3(0)^2)e^{\min\{1,b\}t}$, $t \geq 0$.

4.2 Ocultamento de Dados Através da Sincronização de Caos

4.2.1 Esquemas de Ocultamento

Os trabalhos pioneiros na área de sincronização de Caos levaram a uma série de novas aplicações de caos à comunicação de dados. Tornou-se possível o uso de sistemas caóticos não-autônomos com "sinal" contínuo para transmitir informações. Os mais importantes esquemas de comunicação segura desenvolvidos foram o "Chaotic Masking", o "Chaos Shift Keying" e o "Chaotic Modulation".

Chaotic Modulation

Neste esquema, o codificador consiste em um sistema caótico autônomo cuja saída é adicionada ao sinal de informação. A soma é transmitida pelo canal de comunicação. O decodificador usa o sinal transmitido para sincronizar com um sistema caótico equivalente ao do codificador. O sinal caótico reconstruído é, então, subtraído do sinal recebido. Obtém-se, então, o sinal de informação original.

Mais precisamente, um transmissor deseja enviar um sinal $i(t)$ para um receptor. O transmissor resolve a equação

$$\begin{cases} \dot{u} = f(u, v) \\ \dot{v} = g(u, v) \end{cases}$$

com condições iniciais arbitrárias e envia o sinal $s(t) = i(t) + v(t)$ (ou seja, a soma do sinal da informação com o sinal do subsistema de controle direto). O receptor recebe $s(t)$ e resolve o sistema

$$\begin{cases} \dot{w} = f(w, s(t)) \\ \dot{\tilde{v}} = g(w, \tilde{v}) \end{cases}$$

com outras condições iniciais arbitrárias. Por fim, considera-se $\hat{i}(t) = s(t) - \tilde{v}(t)$. Se $i(t) = 0$, então $v(t) = s(t)$ e a sincronização garante que $|u(t) - w(t)| \to 0$ quando $t \to \infty$. Na prática, trabalha-se com $i(t) \ll s(t)$ e espera-se que ocorra a sincronização, ou seja, $|v(t) - \tilde{v}(t)| \to 0$ quando $t \to \infty$. (Simulações numéricas mostram que a sincronização realmente ocorre se $i(t) \ll s(t)$, embora não existam resultados teóricos a respeito da relação entre $i(t)$ e $s(t)$ para que ocorra a sincronização.)

Uma vez que ocorra a sincronização e $w(t) \approx u(t)$ (para um t arbitrariamente grande), pode-se recuperar o sinal de informação com $\hat{i}(t) = s(t) - \tilde{v}(t)$.

Chaos Shift Keying

Neste esquema o codificador consiste de dois ou mais sistemas caóticos autônomos diferentes. De acordo com o sinal discreto de informação, uma das saídas dos sistemas caóticos é selecionada e transmitida pelo canal. O decodificados possui os mesmos sistemas caóticos que o codificador e, ao receber o sinal por este transmitido, tenta sincronizá-lo com um daqueles sistemas. Os sistemas são escolhidos de forma que ocorra a sincronização de apenas um par. A sincronização indica qual foi a informação discreta originalmente transmitida.

Chaotic Modulation

Também conhecido por Inverse System, neste caso o codificador é um sistema caótico não-autônomo cujo estado é influenciado pelo sinal de informação. O decodificador sincroniza com o codificador através da reconstrução do seu estado usando o sinal transmitido. O sinal de informação é recuperado aplicando a operação inversa ao estado reconstruído e o sinal de transmissão.

4.2.2 Ataques a Sistemas Baseados em Sincronização de Caos

Exemplo de ataque baseado em análise de espectro

Apesar de sistemas caóticos possuírem propriedades que tornam seus sinais de saída bastante similares a um ruído pseudo-aleatório, este tipo de ruído, quando usado em criptografia, deve ter espectro amplo, uniforme, e com potência maior que o sinal que ele irá "camuflar". Em [42] é apresentado um esquema baseado nas equações de Lorenz para ocultar um sinal; o autor deste esquema não considerou a observação acima. O esquema apresentado é descrito pelas seguintes equações:

Transmissor:

$$\begin{cases} \dot{x} = \sigma(y - x,) \\ \dot{y} = rx - y - xz, \\ \dot{z} = xy - bz, \\ s(t) = x(t) + i(t). \end{cases}$$

Receptor:

$$\begin{cases} \dot{y} = rs(t) - y - zs(t), \\ \dot{z} = ys(t) - bz, \\ \hat{i}(t) = s(t) - x(t). \end{cases}$$

onde $i(t)$ é a informação a ser mascarada, $s(t)$ é o sinal transmitido e $\hat{i}(t)$ é a informação recuperada. Para o sistema acima com valores $r = 28$, $\sigma = 10$ e $b = 8/3$ observa-se, após uma análise de espectro, destacados picos de potência nas freqüências $59/2\pi$ Hz e $61/2\pi$ Hz. Conforme mostrado em [44], para recuperar a informação transmitida, basta filtrar as freqüências mencionadas.

Recuperação de parâmetros: ataque de Vaydia e Angadi

Vaydia e Angadi [43] mostram como obter os valores secretos de um criptossistema caótico baseado nas equações de Lorenz. O método consiste de quatro passos. No primeiro passo, determinam-se as derivadas (até a terceira ordem do sinal enviado). O segundo passo é uma transformação da equação que a torna trilinear nos parâmetros. O terceiro passo consiste em remodelar as equações lineares para equações em quatro variáveis. O quarto passo obtém uma inversa generalizada que permite obter os valores das variáveis a partir de simples substituições algébricas.

Formalização do Problema. Em nosso problema, assumimos que um transmissor gera dados usando uma equação diferencial e envia apenas parte dessa informação para o receptor. Por exemplo, temos as equações de Lorenz:

$$\begin{cases} \dot{X} = \sigma(Y - X), \\ \dot{Y} = \rho X - Y - XZ, \\ \dot{Z} = XY - \beta Z, \end{cases}$$

onde as derivadas são tomadas em relação ao tempo. Os parâmetros da equação são σ, ρ e β. O transmissor envia o sinal gerado $X(t)$ para o receptor. Se o receptor conhecer os valores dos parâmetros da equação, é possível reconstituir os sinais de Y e Z usando a sincronização. Questiona-se, então, se é possível obter esses sinais sem o conhecimento prévio dos parâmetros, apenas sabendo-se que o sinal X foi gerado a partir de uma equação de Lorenz.

Passo 1: Forma Canônica. Considere a transformação de X, Y e Z para P, Q e

R, como se segue:

$$\begin{cases} P = X, \\ Q = \rho(Y - X), \\ R = \rho((\rho X - Y - XZ) - \sigma(Y - X)), \end{cases}$$

que terá inversa se $p \neq 0$:

$$\begin{cases} X = P, \\ Y = \dfrac{Q + \sigma P}{\sigma}, \\ Z = \rho - 1 + \dfrac{-Q\sigma - R - Q}{\sigma P}. \end{cases}$$

Com essa transformação, as equações de Lorenz tomam a seguinte forma:

$$\begin{cases} \dot{P} = Q, \\ \dot{Q} = R, \\ \dot{R} = -P^3\sigma - P^2 Q + (\beta\sigma\rho - \beta\sigma)P \\ \qquad\qquad + ((-1 - \sigma)Q\beta + (-\sigma - \beta - 1)R) + \dfrac{QR + Q^2 + Q^2\sigma}{P}. \end{cases}$$

Passo 2: Equação Trilinear. Defina $S = \dot{R}$. Teremos, então:

$$P = X,$$

$$Q = \dot{X},$$

$$R = \ddot{X},$$

$$S = \dddot{X}.$$

Assim, se pudermos estimar com precisão estas derivadas de X em algum ponto, poderemos estimar, também, P, Q, R e S nesse ponto. No entanto, neste ponto, estas quatro quantidades satisfazem à relação:

$$S = -P^3\sigma - P^2 Q + (\beta\sigma\rho - \beta\sigma)P + ((-1 - \sigma)Q\beta + (-\sigma - \beta - 1)R) + \frac{QR + Q^2 + Q^2\sigma}{P}$$

que representa um sistema trilinear em suas variáveis.

Passo 3: Reescrevendo em quatro dimensões. Defina o vetor $F = (F_0, F_1, F_2, F_3)$ da seguinte forma:

$$F_0 = \sigma,$$

$$F_1 = \rho,$$

$$F_2 = \sigma\rho,$$

$$F_3 = \sigma\rho\beta,$$

com

$$\sigma = F_0,$$

$$\rho = F_1,$$

$$\beta = \frac{F_3}{F_2}.$$

O subespaço de R^4 dado pela equação $F_0F_1 - F_2 = 0$ é invariante e poderá ser utilizado para verificar os cálculos.

Passo 4: Formulação Matricial. Assumamos que as derivadas de X são calculadas e, assim, obtemos os valores de P, Q, R e S. Selecione um conjunto de pontos X_n e seus correspondentes P_n, Q_n, R_n e S_n. Defina:

$$G_n = S_n + P_n^2 Q_n + R_n - Q_n \frac{R_n + Q_n}{P_n}$$

e

$$B_{n,0} = \frac{Q_n^2 - P_n^4 - R_n P_n}{P_n}$$

$$B_{n,1} = -(Q_n + R_n)$$

$$B_{n,2} = -(Q_n + P_n)$$

$$B_{n,3} = -P_n.$$

Uma vez calculada a matriz B e o vetor G, a relação com o vetor F é:

$$B_{[n\times 4]} F_{[4\times 1]} = G_{[n\times 1]}.$$

Para obter F de B e G, é necessário inverter B: $F = GB^{-1}$. Uma vez obtido o vetor F, temos os valores dos parâmetros σ, ρ e β, quebrando o código.

Chapter 5

Considerações Finais

5.1 Resumo da Dissertação

Ao longo desta dissertação, conduzimos estudos em três linhas: descrição e análise de cifradores caóticos digitais, relações matemáticas entre caos e criptografia, e aplicações da sincronização de caos à comunicação de dados. Detalharemos o trabalho em cada linha a seguir.

5.1.1 Cifradores Caóticos Digitais

Foi feito um levantamento das principais abordagens para a construção de cifradores caóticos digitais, além da classificação e análise dos cifradores descritos. Foi identificada uma série de problemas com diversos cifradores, tanto com relação a aspectos práticos (por exemplo, viabilidade de implementação e velocidade de encriptação) como com a própria segurança destes cifradores.

A partir do estudo de uma grande quantidade de falhas encontradas em trabalhos sobre cifradores caóticos, foi possível sumarizar estas falhas e criar um conjunto de regras que facilitarão na tarefa de construir cifradores caóticos digitais seguros e práticos.

Também importante para o melhor entendimento do funcionamento desses cifradores é compreender como ocorre a degradação da dinâmica de sistemas caóticos quando estes são implementados em computadores digitais. Esta dissertação identifica como ocorre esta degradação tanto no "curto prazo" quanto no comportamento assintótico, e ainda discute a aplicação do shadowing lemma na implementação de "sistemas caóticos digitais".

5.1.2 Relações Matemáticas entre Caos e Criptografia

As supostas relações entre Caos e Criptografia são há bastante tempo mencionadas por pesquisadores de diversas áreas. Em particular, muito se enfatizou a importância de se desenvolver uma teoria que abrangesse ambas as disciplinas, que permitiria estudar as propriedades criptográficas de sistemas caóticos e as propriedades dinâmicas de transformações criptográficas. No entanto, poucos pesquisadores tentaram conduzir suas pesquisas nesse caminho.

Nesta dissertação, buscamos investigar essas "conexões" através do estudo das propriedades dinâmicas de criptossistemas. Adaptando conceitos de teoria da medida e teoria ergódica para o domínio da criptografia, foi possível definir de forma mais clara algumas de suas propriedades e relacioná-las com propriedades de sistemas caóticos.

Ao final do capítulo, foi possível alcançar um interessante entendimento das propriedades de difusão e confusão de criptossistemas relacionando-as com propriedades de sistemas dinâmicos. A primeira idéia principal relaciona a difusão com a propriedade de que a incerteza sobre o estado do sistema não pode ser aproximada pelo conhecimento de um estado anterior, ou seja, o comportamento do sistema é "puramente probabilístico". A segunda idéia principal é que, uma vez que a difusão "garante" um comportamento probabilístico do sistema, a confusão "garante" que a

análise das estatísticas deste sistema não forneça informações sobre ele.

5.1.3 Sincronização de Caos e Comunicação

Fizemos um levantamento histórico dos avanços em sincronização do caos e de suas aplicações à comunicação segura de dados. Analisamos uma grande quantidade de trabalhos, identificando suas características e as principais classes de ataques aos sistemas de comunicação baseados em sincronização.

5.2 Novos Caminhos

A disciplina da Criptografia é muito focada em aplicações - de fato, a maioria das publicações da área é voltada para a construção e análise de criptossistemas, sem a investigação rigorosa de seus princípios matemáticos. Assim, a criptografia possui uma série de lacunas em sua "teoria matemática" que inspiram novos e interessantes problemas. O estudo conjunto de Sistemas Dinâmicos e Criptografia parece ser um possível caminho para a investigação destes problemas matemáticos, devido às semelhanças entre conceitos de ambas as áreas. No que se segue, apresentamos sugestões do que parecem ser os principais caminhos para pesquisa na área de Caos e Criptossistemas.

5.2.1 Futuros Trabalhos a partir desta Dissertação

Como mencionamos, uma das grandes dificuldades na condução deste trabalho foi a ausência de ferramentas matemáticas para o estudo da Criptografia; muitas vezes, conceitos fundamentais não haviam sido estabelecidos. Acreditamos que esta dissertação já representou um passo no sentido de estabelecer algumas conexões conceituais entre propriedades da Criptografia e de Sistemas Dinâmicos. No entanto, o

tempo disponível para a elaboração deste trabalho não permitiu que tais "avanços conceituais" pudessem ser consolidados na forma de uma teoria matemática rigorosa. Ainda assim, acreditamos que belos trabalhos matemáticos poderão ser elaborados a partir de pesquisas mais aprofundadas (e mais rigorosas) nos tópicos mencionados a seguir:

Definição Precisa dos Conceitos de Confusão e Difusão

Nesta dissertação apresentamos uma nova proposta para o entendimento das propriedades de difusão e confusão de um criptossistema, relacionando-os com propriedades ergódicas de sistemas dinâmicos. No entanto, esses conceitos ainda carecem de uma definição matemática rigorosa. A investigação dos conceitos de difusão e confusão em sistemas dinâmicos contínuos é um tópico que pode gerar interessantes e úteis trabalhos.

Nova Classe de Ataques a Criptossistemas: "Known-Statistics"

A investigação das propriedades ergódicas de criptossistemas levou naturamente à elaboração de uma nova classe de ataques a criptossistemas, em que se pode determinar a probabilidade "a priori" da linguagem utilizada para comunicação. Essa classe descreve ataques bastante plausíveis e, até onde o autor tem conhecimento, nunca fora descrita ou investigada. O estudo aprofundado desta classe de ataques e a análise de criptossistemas práticos ou teóricos sob ataques deste tipo poderá fornecer material para muitos trabalhos na área de criptografia.

Sistematização de ataques ao criptossistemas baseados em sincronização

Até o momento a maioria dos trabalhos de criptanálise de sistemas baseados em sincronização do caos se dedicou a ataques "ad hoc". Muitos ataques criativos foram

elaborados, no entanto ainda não se possui métodos gerais de ataques. Como exemplo, o ataque de "determinação de parâmetros" descrito ao final do capítulo 3 é extremamente interessante e bem-sucedido, mas se aplica a criptossistemas caóticos baseados nas equações de Lorenz. Não existem resultados que caracterizem os sistemas contra os quais tal ataque pode ser aplicado. Um trabalho interessante a ser elaborado é a continuação da identificação e classificação de ataques iniciada nesta dissertação, seguida da descrição precisa das características de cada uma dessas classes e da caracterização dos criptossistemas contra os quais tais ataques podem ser aplicados com sucesso.

5.2.2 Outros Caminhos Sugeridos

Novas Abordagens para o Projeto de Cifradores Caóticos Digitais

O uso de caos em cifradores digitais deu origem a novas abordagens para a definição de funções de encriptação, como, por exemplo, os cifradores baseados em busca, que usa a técnica bastante inovadora de buscar partes da mensagem-plana em trajetórias caóticas. Apesar de interessante, essa abordagem mostrou-se pouco prática. A pesquisa de novas técnicas e abordagens para cifradores caóticos digitais deverá focar-se na construção de criptossistemas seguros e eficientes.

Propriedades Dinâmicas de Criptossistemas

Este foi o principal tópico de pesquisa desta dissertação. Esta é uma tentativa de se fazer uma investigação matemática rigorosa das propriedades dinâmicas de criptossistemas e relacioná-las com conceitos de Teoria do Caos. Esse tipo de investigação poderá dar origem, em algum momento, a uma teoria matemática mais rigorosa da

criptografia, e que possibilitará uma compreensão maior da segurança de criptossistemas.

A investigação dessas propriedades dinâmicas de criptossistemas é feita inspirada na Teoria da Medida, Teoria Ergódica e Teoria do Caos, mas com seus conceitos "transpostos" para o domínio discreto. Por este motivo, a Matemática Combinatória tem papel importante nestas "investigações. O autor tem plena convicção de que a pesquisa matemática rigorosa das propriedades da criptografia dará origem a questões interessantíssimas e proporcionará o surgimento de belos trabalhos e idéias.

Criptografia do Contínuo

Assim como o estudo das propriedades dinâmicas de criptossistemas se mostrou um tópico de bastante interesse, também são interessantes as questões a respeito da análise de transformações caóticas do ponto de vista da criptografia. A extensão de conceitos como difusão e confusão para o domínio contínuo possibilitarão a construção de criptossistemas definidos em domínio contínuo. Embora o conceito seja, de certa forma, uma abstração, as teorias de computabilidade do contínuo podem vir a, um dia, tornar aplicáveis as idéias deste campo de pesquisa.

Dinâmica do "Caos Digital"

Ao mesmo tempo em que os conceitos de criptografia ainda não foram adequadamente estendidos de forma a abranger domínios contínuos, os conceitos e idéias da teoria do Caos não fazem sentido quando transpostos para domínios discretos. Qualquer sistema definido em um domínio discreto, assumindo, assim, um número finito de estados, eventualmente irá repetir um deles e, dessa forma, iniciar um ciclo periódico.

A existência de tal ciclo impede que classifiquemos o sistema como caótico, independente de quão complexo for o seu "movimento" dentro daquele ciclo.

Este tópico tem aplicações imediatas para que se alcance a plena compreensão de cifradores digitais. Como estes cifradores utilizam a reprodução digital de sistemas caóticos, é importante

1) entender que tipo de degradação ocorre na dinâmica destes sistemas "discretizados" em relação à sua versão contínua, e

2) desenvolver métodos de recuperação (ainda que parcial) em computador da dinâmica do sistema caótico.

Citamos, ao longo do texto, o exemplo da técnica de pequenas perturbações, desenvolvida para auxiliar na determinação da densidade invariante de sistemas caóticos e que já é utilizada para a implementação de sistemas digitais com dinâmica mais complexa, os quais são aplicados à criptografia digital.

Em todo caso, sistemas discretos com comportamento dinâmico complexo têm recebido muita atenção e seus campos de aplicação variam da biologia teórica à gravitação quântica. Redes neurais assimétricas, como as estudadas em [22] podem ter comportamentos extremamente complicados, associados ao conceito de caos, enquanto autômatos celulares apresentam bifurcações em diversos regimes, os mais desordenados dos quais têm sido descritos como caóticos. Ainda não está claro, no entanto, como este tipo de dinâmica está relacionado ao caos determinístico no espaço de fase Euclidiano.

5.3 Conclusão

Neste trabalho analisamos as aplicações da matemática do contínuo, mais específicamente dos Sistemas Dinâmicos, à disciplina de Teoria da Criptografia, um campo de estudo eminentemente regido pela matemática discreta. Observamos que uma grande quantidade dos trabalhos em sistemas dinâmicos voltados para criptografia, especialmente os trabalhos iniciais (décadas de 1980 e 1990), consistiu simplesmente na construção ad hoc de criptossistemas que, de alguma forma, utilizavam idéias associadas a Sistemas Dinâmicos.

Essa abordagem inicial mostrou-se bastante improdutiva. Por um lado, deixava-se de explorar as interessantes questões matemáticas levantadas ao se confrontar as idéias da Teoria da Criptografia com aquelas da Matemática do Contínuo. Por outro lado, freqüentemente os matemáticos responsáveis por estes primeiros estudos não possuíam conhecimentos aprofundados em Criptografia, de forma que acabavam construindo criptossistemas fracos, o que levou ao desinteresse da comunidade de Criptografia pelo uso das ferramentas da Matemática do Contínuo. De todo modo, não podemos deixar de valorizar os esforços que levaram a estes primeiros trabalhos, que abriram caminho para o que hoje promete ser uma fonte de boas ferramentas para a Criptografia e de interessantes problemas matemáticos.

Atualmente verifica-se uma modificação da abordagem dos matemáticos que abordam temas de Criptografia. Já se faz criptoanálise dos criptossistemas propostos, o que tem levado a um maior interesse da comunidade de Criptografia. Observa-se o surgimento de criptossistemas com a efetiva utilização de conceitos e idéias de Sistemas Dinâmicos e que são bastante resistentes aos ataques de criptoanálise. Assim, no campo da "prática", o futuro próximo dos "criptossistemas caóticos" é bastante

promissor.

Com relação aos aspectos matemáticos da criptografia, ainda há muito a explorar. A maioria dos trabalhos não tem se proposto a analisar - ou mesmo menciona - os interessantes problemas de transposição dos conceitos de criptografia (como, por exemplo, os de segurança, confusão e mistura) para o domínio do contínuo e as questões de reinterpretação de conceitos eminentemente contínuos (como o caos) nos domínios discretos.

Esperamos que esta dissertação possa ser utilizada como um ponto de partida para o estudo das relações entre sistemas dinâmicos e criptossistemas, além de suas aplicações. Uma grande quantidade de estudos e abordagens está aqui descrita, de forma que o leitor poderá ter uma visão muito ampla de toda a atividade que está sendo conduzida na área. Além disso, a grande quantidade de referências irá permitir o acesso a pesquisas mais aprofundadas. Esperamos que o leitor desta dissertação, ao partir para buscar novas fontes de informação, possa ter uma percepção do amplo espectro de interessantes problemas que se abrem ao confrontarmos problemas da matemática discreta - Criptografia - com problemas da matemática do contínuo - Sistemas Dinâmicos.

Referencias

[1] Mañe. Ergodic Theory and Differentiable Dynamics. Springer-Verlag, 1948.

[2] C. E. Shannon. A Mathematical Theory of Communication, *Bell Systems Tech. J.*, 27(3), 379-423, 1948.

[3] C. E. Shannon. Communication Theory of Secrecy Systems, *Bell Systems Tech. J.*, 28(3), 656-715, 1949.

[4] Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. IEEE Trans. on Inform. Theor. IT-22, 6 (Nov.), 644-654, 1976.

[5] Y. Pesin. Characteristics exponents and smooth ergodic theory, Russian Math. Surveys. 32, 55-114, 1977.

[6] P. Collet, J. P. Eckmann. Iterated maps on the interval as dynamical systems. Birkhäuser, Basel, 1980.

[7] D. Knuth. The Art of Computer Programming, vol.2, Seminumerical Algorithms, 2^a ed., Addison-Wesley, Reading, Massachusetts, 1981.

[8] A. Yao. Theory and Applications of Trapdoor Functions. IEEE 23rd Symp. Found. Comp. Sci. 80-91, 1982.

[9] Stephen Wolfram. Cryptography with cellular automata, Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85, 429-432, 1985.

[10] Puhua Guan. Cellular Automaton Public-Key Cryptosystem, Complex Systems, 1:51-57, 1987.

[11] R. Matthews. On the Derivation os a "chaotic" encryption algorithm, Cryptologia, XIII(1):29-42, 1989.

[12] R. L. Devaney. An Introduction to Chaotic Dynamical Systems, 2nd Edition, Addison-Wesley Publishing Company, Reading, MA, 1989.

[13] G. M. Bernstein, M. A. Lieberman. "Secure random number generation using chaotic circuits," IEEE Trans. Circuits Syst., vol.37, 1157-1164, 1990.

[14] L. M. Pecora e T. L. Carrol, Synchronization in chaotic systems, Physical Review Letters, 64(8):821-824, 1990.

[15] Edward Ott, Celso Grebogi, James A. Yorke. Controlling Chaos, Physical Review Letters, 64(11):1196-1199, 1990.

[16] Scott Hayes. Communicating with Chaos, Physical Review Letters, 70(20):3031-3034, 1990.

[17] T. Habutso, Y. Nishio, I. Sasase, S. Mori. A secret key criptosystem using chaotic map, Trans. IEICE, E 73(7):1041-1044, 1990.

[18] R. Forre. The Henon attractor as a keystream generator. Advances in Cryptology – EuroCrypt'91, Lecture Notes in Computer Science vol.0547, 76-81. Spinger-Verlag, Berlin, 1991.

[19] Eli Biham. Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91, Proceedings of EUROCRYPT'91, 1991.

[20] T. Habutso, Y. Nishio, I. Sasase, S. Mori. A secret key criptosystem by iterating chaotic map, Advances in Criptology - EuroCrypt'91, Lecture Notes in Computer Science vol. 0547, 127-140, Springer-Verlag, Berlin, 1991.

[21] Douglas R. Frey. Chaotic Digital Encoding: An Approach to Secure Communication. IEEE Trans. Circuits Syst. II vol. 40, no 10, pp. 660-666, Oct. 1993.

[22] Crisanti A., Falcioni M., Vulpiani A.. Transition from Regular to Complex Behavior in a Discrete Deterministic Asymmetric Neural Network Model. J. Phys. A: Math. Gen. 26 / 3441, 1993.

[23] B. Schneier. Fast Software Encryption, Cambridge Security Workshop Proceedings (1993), Springer-Verlag, pp. 191-204, 1994.

[24] T. L. Carroll, L. M. Pecorra. Synchronising Chaotic Circuits. IEEE Trans. Circuits Syst. vol. 38, no 8, pp. 191-196, 1995.

[25] Tohru Kohda, Akio Tsuneda. Chaotic bit sequences for stream cipher cryptography and their correlation functions. Chaotic Circuits for Communication, Proceedings of SPIE vol.2612, 86-97, 1995.

[26] Ute Feldmann, Martin Hasler, Wolfgang Schwarz. Communication by chaotic signals: The inverse system approach. Int. J. Circuit Theory and Applications, 24(5):551-579, 1996.

[27] Marco Götz, Kristina Kelber, Wolfgang Schwarz. Discrete-time chaotic encryption systems - Part I: Statistical design approach. IEEE Trans. Circuits and Systems-I, 44(10):963-970, 1997.

[28] Frank Dachselt, Kristina Kelber. Discrete-time chaotic encryption systems - Part III: Cryptographycal Analysis. IEEE Trans. Circuits and Systems-I, 45(9):983-988, 1998.

[29] M. S. Baptista. Cryptography with Chaos. Physics Letters A, 240:50-54, 1998.

[30] Kiri Fridrich. Symmetric Ciphers based on two-dimentional chaotic maps. Int. J. Bifurcation and Chaos, 8(6), 1259-1284, 1998.

[31] Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows. J. Electronic Imaging, 7(2), 318-325, 1998.

[32] Ljupčo Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In Proc. IEEE Int. Symposium Circuits and Systems, volume 4, 514-517. IEEE, 1998.

[33] Masaki Miyamoto, Kiyoshi Tanaka, Tatsuo Sugiruma. Truncated baker transformation and its extension to image encryption. Proc. SPIE vol. 3814, 13-25, 1999.

[34] E. Alvarez, A. Fernandez, P. Garca, J. Jimenez, A. Marcano. New approach to chaotic encryption, Phys. Lett. A 263 (1999) 373-375.

[35] G. Alvarez, F. Montoya, M. Romera, G. Pastor. Cryptoanalysis of a chaotic encryption system. Physics Letters A, 276:191-196, 2000.

[36] Ljupčo Kocarev. Chaos-based Cryptography: A brief overview. IEEE Circuits and Systems Magazine, 1(3):6-21, 2001.

[37] Goce Jakimoski, Ljupčo Kocarev. Chaos and Cryptography: Block Encryption Chiphers Based on Chaotic Maps. IEEE Trans. Circ. Syst. I, 48(2):163-169, 2001.

[38] Ljupčo Kocarev, Goce Jakimoski. Logistic map as a block encryption algorithm. Physics Letters A, 289(4-5):199-206, 2001.

[39] Goce Jakimoski, Ljupčo Kocarev. Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Trans. Circuits and Systems–I, 48(2):163-169, 2001.

[40] Shujun Li, Xuan Zheng, Xuanqin Mou and Yuanlong Cai. "Chaotic Encryption Scheme for Real-Time Digital Video," in: Real-Time Imaging VI (part of proceedings of IS&T/SPIE's 14th Annual Symposium on Electronic Imaging, 20-25 January, 2002, San Jose, CA), Proceedings of SPIE, vol. 4666, 149-160, 2002

[41] X Yi, C H Tan, C K Siew. "A New Block Cipher Based on Chaotic Tent Map", IEEE Trans. on Circuits and Systems Part I, Vol 49, no.12, pp. 1826-1829, 2002.

[42] Q. Memon. Synchronized chaos for network cryptography, Computer Communications 26 / 498-505, 2003.

[43] P.G. Vaidya, Savita Angadi. Decoding chaotic cryptography without access to the superkey; Chaos, Solitons and Fractals 17, 379-386, 2003.

[44] Gonzalo Álvarez, Shujun Li. Breaking network security based on chaos synchronization. Computer Communications 27, 1679-1681, 2004.

[45] F. Dachselt, W. Schwarz. Chaos and Cryptography, IEEE Trans. Circ. Systems I, 48(12):1498-1509.

[46] Shujun Li, Xuanquin Mou, Yuanlong Cai. Chaotic Cryptography in Digital World: State-of-the-art, Problems and Solutions.

[47] Henri Waelbroeck, Federico Zertuche. Discrete Chaos.

[48] Ninan Sajeet Philip, K. Babu Joseph. Chaos for Stream Cipher. Cochin University of Science and Technology.

[49] Andrzej Lasota, Michael C. Mackey. Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics (Applied Mathematical Sciences).

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo