PROPOSTA DE FORTALECIMENTO DO SISTEMA CRIPTOGRÁFICO DES CONTRA CRIPTOANÁLISE DIFERENCIAL

José Carlos Fontoura Guimarães

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA A OBTENÇÃO DE GRAU DE MESTRE

Área de Concentração : Ciência da Computação
Orientador: Prof. Dr. Routo Terada

São Paulo, março de 1993

Aos meus pais e avós

À Valentina por sua paciência, compreensão e estímulo nas horas difíceis

Agradecimentos

Ao Professor Routo Terada pela orientação, apoio e incentivo.
A CAPES pelo apoio financeiro recebido.
A todas as pessoas que contribuíram direta ou indiretamente para a conclusão deste trabalho.

Abstract

We propose a new version of 16-round DES in which a probabilistic swapping is used to strengthen DES against differential cryptanalysis. This new cipher system, called SWDES, decreases the probability of success in a differential cryptanalysis attack by reducing the probability of the characteristics that are used against DES. Encryption and decryption speed of SWDES is almost the same as that of 16-round DES.

Resumo

Apresentamos uma nova versão do DES com 16 iterações no qual uma troca probabilística é utilizada para fortalecer o DES contra criptoanálise diferencial. Este novo criptossistema, chamado SWDES, diminui a probabilidade de sucesso de um ataque por criptoanálise diferencial através da redução das probabilidades das características utilizadas contra o DES. O tempo de ciframento e deciframento do SWDES é semelhante ao do DES com 16 iterações.

Conteúdo

Prefácio

O objetivo deste trabalho é apresentar uma proposta de alteração no sistema criptográfico DES (Data Encryption Standard) [NBS77]. Este sistema criptográfico foi projetado pela IBM para o governo americano para uso geral em transações bancárias, comunicações sigilosas entre empresas, etc [Pf89]. Devido ao aval dado pelo governo americano, o DES tornou-se amplamente utilizado em inúmeras aplicações por todo o mundo. Posteriormente este aval foi retirado em 1987, gerando muitas dúvidas quanto à segurança deste sistema.

Desde a sua invenção, o DES tem sido alvo dos criptoanalistas e recentemente, dois cientistas israelenses, Biham e Shamir publicaram um ataque relativamente rápido a este sistema, utilizando uma técnica denominada Criptoanálise Diferencial [BS90,91,92].

O DES é um criptossistema projetado para ser utilizado em hardware, o que torna a sua implementação em software ineficiente. Consequentemente originou-se um grande parque instalado de máquinas que utilizam este sistema, tornando sua completa substituição a curto prazo economicamente inviável. Portanto a pesquisa de alterações que fortaleçam o DES contra o ataque por Criptoanálise Diferencial e que não exijam grandes alterações nos equipamentos existentes, mas que mantenham a eficiência do sistema, torna-se economicamente interessante.

Este trabalho está organizado em quatro capítulos e dois apêndices. No capítulo 1 são apresentados alguns conceitos básicos de criptografia e o algoritmo do DES. Algumas fraquezas deste sistema criptográfico também são mostradas. O capítulo 2 contém a base teórica para o desenvolvimento e análise da proposta de alteração. Apresentamos os conceitos de Criptoanálise Diferencial, criptossistemas de Markov, características, e probabilidades diferenciais. O capítulo 3 apresenta a proposta de alteração (o algoritmo SWDES) e as propriedades que este sistema possui. Apresentamos os resultados de alguns experimentos realizados e mostramos uma comparação deste sistema com o sistema DES padrão. No capítulo 4 apresentamos as conclusões deste trabalho, incluindo comentários sobre a viabilidade econômica de implementação do SWDES. Finalmente os apêndices A e B contém respectivamente as tabelas de permutações, expansões e caixas de substituição correspondentes ao DES; e os resultados de alguns experimentos realizados com o SWDES que estão também representados graficamente no capítulo 3.

Capítulo 1

Criptografia e o DES

1.1 Conceitos Fundamentais

Criptografia (do grego kryptós = oculto + grápho = escrita) corresponde a um conjunto de técnicas que permitem cifrar (ou codificar) uma mensagem, originalmente escrita de forma clara e perfeita, em um texto incompreensível de modo que apenas o destinatário consiga decifrar (ou decodificar) este texto e recuperar a mensagem original [Lu86]. Neste texto denotaremos por **mensagem** um texto que se deseja cifrar e por **criptograma** um texto cifrado.

A transformação de uma mensagem em criptograma chama-se **ciframento.** A transformação de um criptograma em mensagem chama-se **deciframento**

A Criptografia possui muitas aplicações. É utilizada, por exemplo, em ambientes de guerra e em comunicações entre embaixadas. Mas não se restringe a estes fins. Com o surgimento de grandes redes de computadores em que um grande número de pessoas compartilham um mesmo sistema, a necessidade de proteção de arquivos e segurança na transmissão de dados tornou-se muito importante.

Um **sistema criptográfico** ou **criptossistema** consiste numa seqüência de operações (ou algoritmo) que permitem que uma mensagem seja reescrita (operação de ciframento) de tal forma que apenas o destinatário possa restaurar a mensagem original (operação de deciframento).

A **chave** num sistema criptográfico é um parâmetro introduzido com a mensagem original no algoritmo de ciframento (chave de ciframento) e com a mensagem cifrada no algoritmo de deciframento (chave de deciframento), de tal forma que a obtenção de uma mensagem cifrada a partir de uma mensagem original ou o procedimento inverso não dependa apenas dos algoritmos de ciframento e deciframento mas também das chaves utilizadas. A existência de chaves permite que, mesmo sendo conhecidos os algoritmos de ciframento e deciframento, apenas quem as possui pode cifrar ou decifrar mensagens utilizando um dado sistema criptográfico.

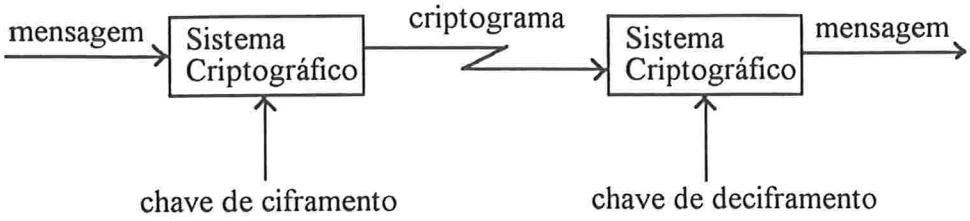


Figura 1.1a: Esquema de um sistema criptográfico

Um sistema criptográfico é **assimétrico** quando a chave de deciframento é diferente da chave de ciframento e a chave de deciframento não pode ser calculada facilmente através da chave de ciframento. Pelas características deste sistema, um usuário X, por exemplo de um correio eletrônico, pode ter uma chave de ciframento pública e uma chave de deciframento secreta, permitindo que vários outros usuários possam enviar-lhe mensagens cifradas utilizando para isto sua chave de ciframento, que é pública. Porém apenas X pode decifrá-las pois ele é o único possuidor da chave de deciframento que não pode ser obtida a partir da chave de ciframento de maneira computacionalmente viável. Por esta razão o sistema criptográfico assimétrico também é chamado de sistema criptográfico de chave pública. Um exemplo de sistema criptográfico assimétrico é o RSA [RS78].

Um sistema criptográfico é **simétrico** quando a chave de deciframento é igual à chave de ciframento ou quando a chave de deciframento pode ser facilmente obtida através da chave de ciframento. O sistema criptográfico DES [NBS77] é simétrico.

Neste trabalho só focalizaremos sistemas simétricos.

1.2 O Sistema Criptográfico DES

O sistema criptográfico DES (Data Encryption Standard) cifra mensagens de 64 bites de comprimento em criptogramas de igual tamanho utilizando uma chave de ciframento de 56 bites de comprimento. A chave de ciframento que é fornecida externamente possui tamanho de 64 bites porém apenas 56 bites são efetivamente utilizados pelo sistema. Os 8 bites restantes podem ser utilizados para verificação de paridade.

O processo de ciframento consiste em 16 iterações onde cada iteração utiliza uma função de ciframento denominada F e uma subchave Ki obtida a partir da chave de ciframento . O conjunto de subchaves utilizadas é denotado por K1, K2,..., K16. O processo de ciframento está ilustrado na Figura 1.2a.

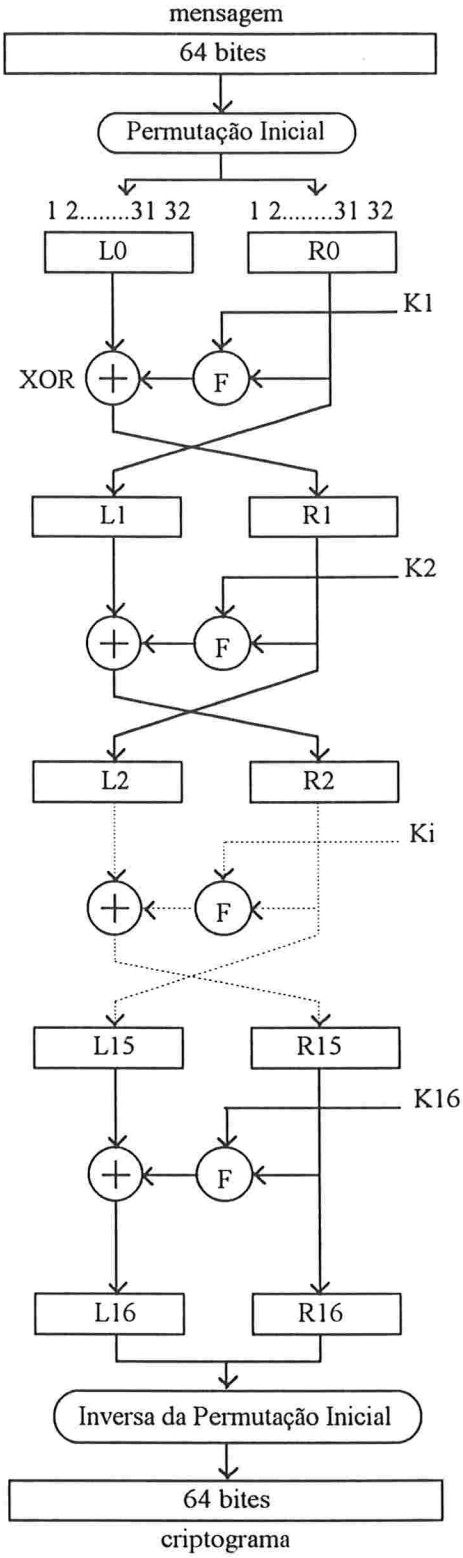


Figura 1.2a: Esquema de ciframento do DES

O esquema de geração das 16 subchaves está representado na Figura 1.2b. Basicamente o processo consiste nos seguintes passos:

(i) Aplicar a Permutação Escolha 1* à chave de 64 bites obtendo uma palavra de 56 bites (CD);

(ii) Dividir CD em duas metades de 28 bites C e D;

(iii) Aplicar a cada metade de 28 bites deslocamentos circulares à esquerda. O número de deslocamentos aplicados varia em cada iteração de acordo com a Tabela A1 (vide Apêndice A);

(iv) Compor as duas metades em uma palavra de 56 bites (CD) e aplicar a esta palavra a Permutação Escolha 2, obtendo-se então uma subchave;

(v) Repetir os passos (ii), (iii) e (iv) para as subchaves restantes.

Os passos executados pelo algoritmo de ciframento do DES são os seguintes:

(i) Aplicar à mensagem a Permutação Inicial;

(ii) Dividir a entrada em 2 metades L (esquerda) e R (direita);

(ii) Executar 16 iterações caracterizadas da seguinte forma:

Cada iteração (com exceção da última) pode ser dividida em duas partes: Tr e Sw (vide Figura 1.2c).

Tr é uma transformação que depende de uma subchave de 48 bites e que preserva a metade direita (R). Esta transformação consiste de:

(a) uma função F aplicada à metade direita (R) e que depende de uma subchave de 48 bites. F consiste em uma expansão (E) de 32 bites para 48 bites, uma operação de OU-Exclusivo (XOR[1]) com uma subchave de 48 bites, uma contração de 48 bites para 32 bites (também chamada de substituição) através de 8 contrações de 6 bites para 4 bites (utilizando as Caixas de Substituição S1, S2,...e S8) e uma permutação (P) de 32 bites (vide Figura 1.2d);

(b) uma aplicação de XOR entre a saída de F e a metade esquerda (L).

Sw é uma troca de duas metades de 32 bites de comprimento . Na última iteração Sw não é realizada.

(iii) Combinar as metades L e R de 32 bites cada em uma palavra de 64 bites;

(iv) Aplicar a Inversa da Permutação Inicial à palavra de 64 bites, obtendo-se então o criptograma.

---

* O apêndice A contém as tabelas correspondentes às permutações, expansões e compressões realizadas no DES

[1] a XOR b = a ⊕ b = (a+b) mod 2 = resto da divisão de (a+b) por 2

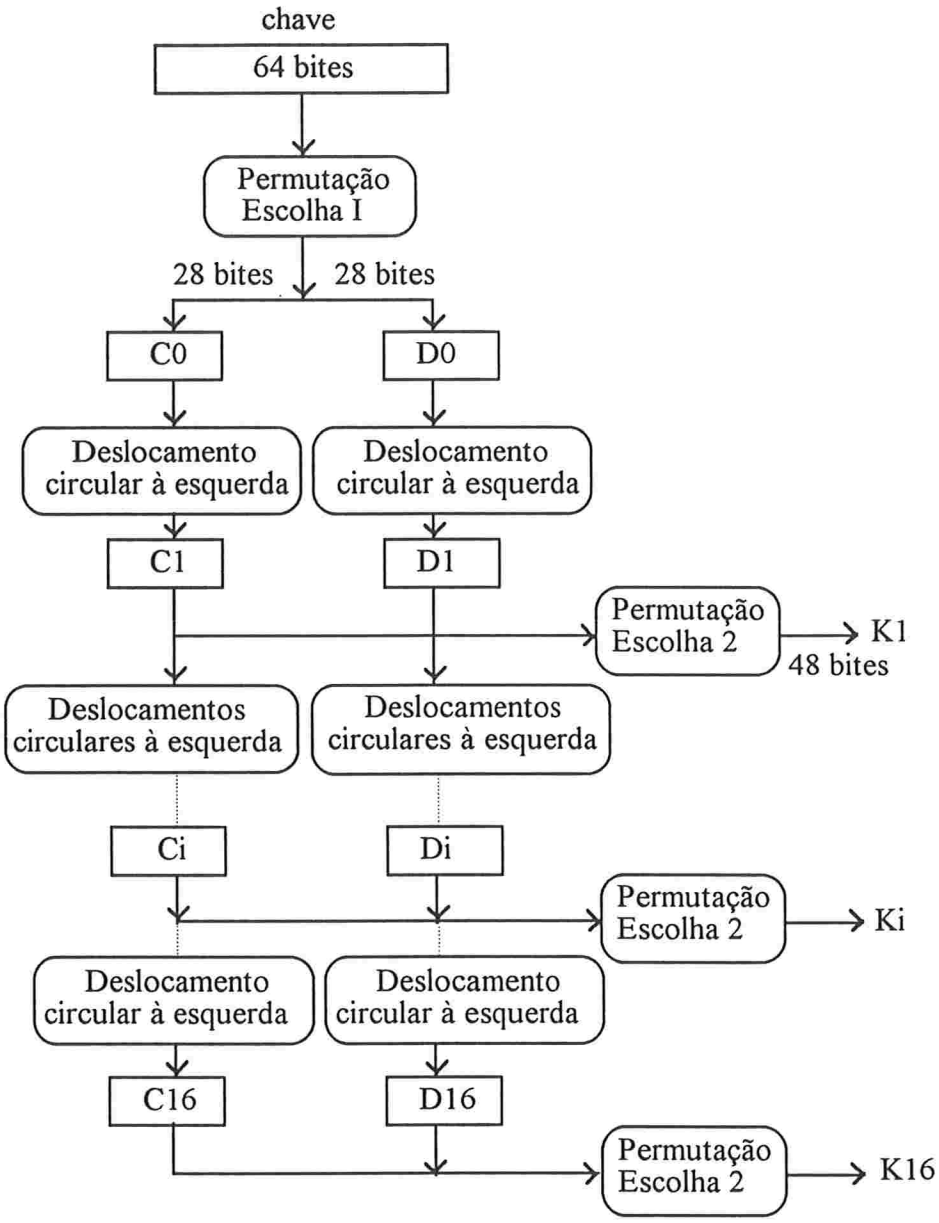


Figura 1.2b: Esquema de geração das subchaves

O DES implementa dois conceitos da Teoria de Informação de Shannon [Sh49] : **confusão** e **difusão**. Implementa-se a confusão quando a mensagem é alterada de modo que o criptograma não possua uma relação óbvia com a mensagem. Implementa-se a difusão ao se garantir que o efeito de um bit na mensagem atinge vários outros bites do criptograma. As caixas de substituições implementam a confusão através da modificação do padrão de bites. As permutações implementam a difusão através do reordenamento dos bites [Pf89]. Ambos os conceitos podem ser agrupados em um único termo chamado **efeito avalanche**, isto é, uma pequena modificação na mensagem provoca uma grande alteração no criptograma [K81].

A Figura 1.2a pode ser representada da seguinte forma:
$DES = IP^{-1} \bullet Tr_{K16} \bullet Sw \bullet Tr_{K15} \bullet ... \bullet Sw \bullet Tr_{K2} \bullet Sw \bullet Tr_{K1} \bullet IP$

Sw é uma involução pois Sw^2 = Identidade. Tr também é uma involução:
$Tr(L_i,R_i) = (L_i \oplus F(R_i,K_{i+1}), R_i)$.
$Tr^2(L_i,R_i) = (L_i \oplus F(R_i,K_{i+1}) \oplus F(R_i,K_{i+1}), R_i) = (L_i,R_i)$. Portanto o processo de deciframento é essencialmente idêntico ao de ciframento, apenas inverte-se a ordem de utilização do conjunto de subchaves: K16, K15, ..., K1 (vide Figura 1.2e):
$DES^{-1} = IP^{-1} \bullet Tr_{K1} \bullet Sw \bullet Tr_{K2} \bullet ... \bullet Sw \bullet Tr_{K15} \bullet Sw \bullet Tr_{K16} \bullet IP$

Todas as tabelas correspondentes às permutações, expansões e compressões realizadas pelo algoritmo do DES são apresentadas no Apêndice A.

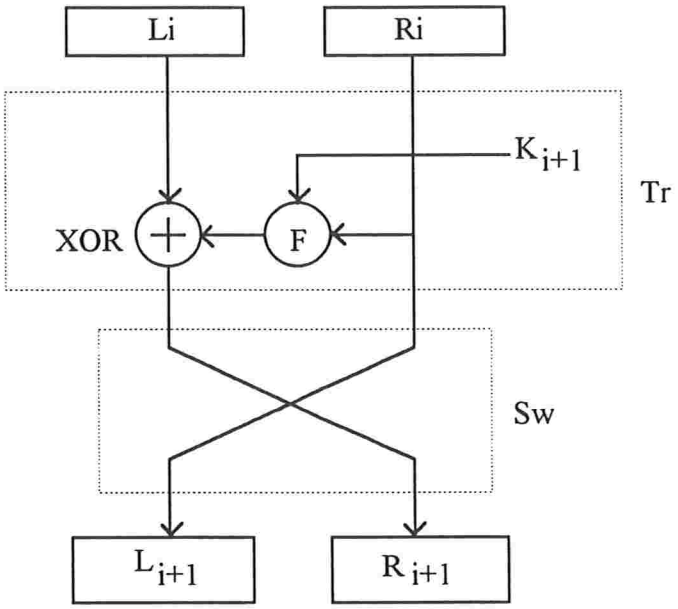


Figura 1.2c: Partes de cada iteração do processo de ciframento

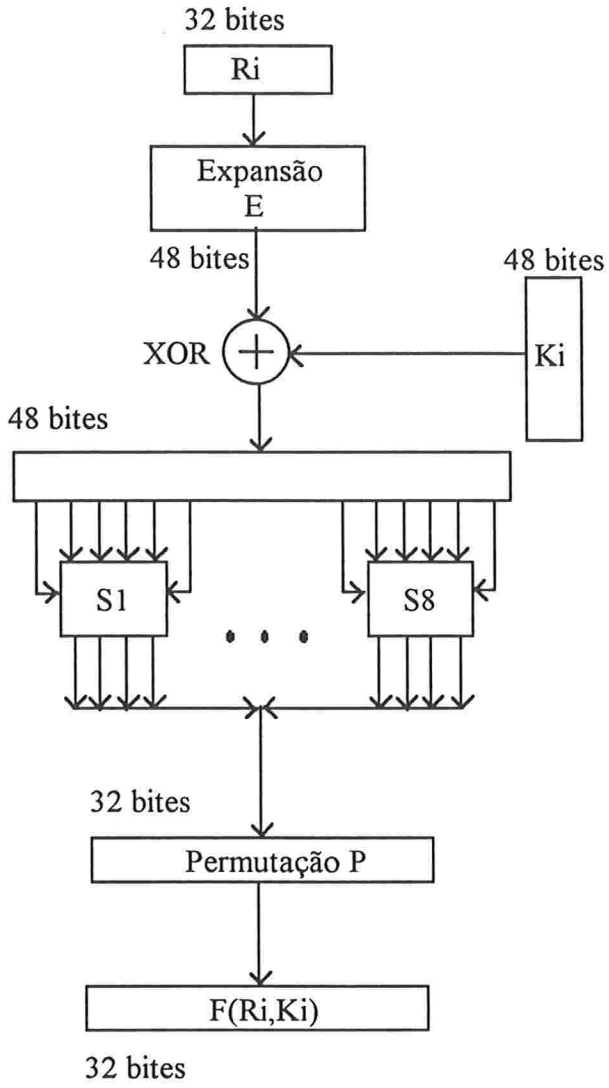


Figura 1.2d: Detalhe de funcionamento da função F

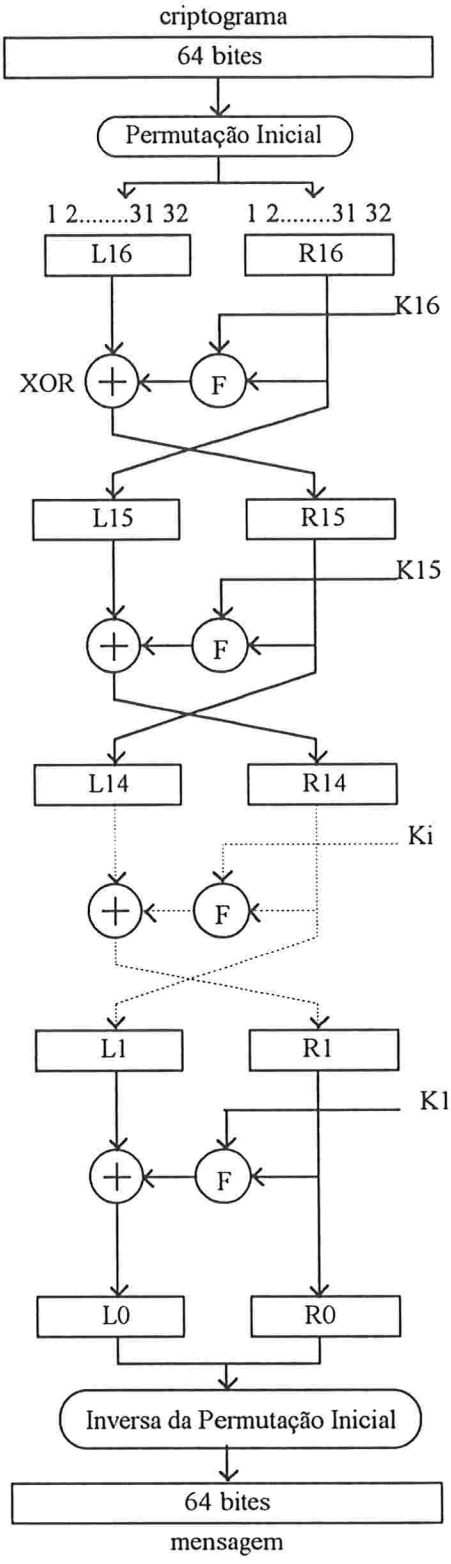


Figura 1.2e: Esquema de deciframento do DES

1.3 Algumas Fraquezas Conhecidas do DES

Apresentamos a seguir algumas fraquezas conhecidas do DES: Complementaridade, Existência de Chaves Fracas, Existência de Chaves Semi-Fracas e Colisão de Chaves [Da81, DQ84, Pf89].

1.3.1 Complementaridade

Inicialmente vamos introduzir a seguinte notação: seja X um número binário. $\overline{X}$ denota o Complemento de Um* de X.

Seja **M** uma mensagem e **K** uma chave de ciframento para o DES. Seja **C** o criptograma obtido cifrando-se M: $C = DES(K, M)$.

O número de chaves possíveis no DES é 2^{56} pois o número de bites efetivamente utilizados pelo algoritmo de ciframento é 56. Este é o número de chaves que, no pior caso, teríamos que tentar para obtermos K tendo-se em mãos M e C. Para tal deveríamos cifrar M com todas as chaves possíveis e comparar qual o criptograma que é idêntico a C (este procedimento é denominado busca exaustiva). Porém o DES possui a seguinte característica: $\overline{C} = DES(\overline{K}, \overline{M})$. Isto reduz o número de chaves que se precisa verificar pela metade, caso se consiga obter o resultado do ciframento de $\overline{M}$ com a mesma chave K. Para verificarmos isto, vamos analisar o seguinte procedimento: Sejam C, M, K e C_2 tais que $C = DES(K, M)$, K é a chave que se deseja descobrir e $C_2 = DES(K, \overline{M})$.

Para cada chave T possível repita
Início
    $Y = DES(T, M)$;
    Se Y=C Então K=T;
    Senão Se Y= $\overline{C}_2$ Então K=$\overline{T}$ **;
Fim

---

* o Complemento de Um de um número binário é obtido trocando-se todos os 0's por 1's e 1's por 0's. Por exemplo, o Complemento de Um de 1001011 é 0110100.

** $\overline{C}_2 = DES(\overline{K}, \overline{\overline{M}}) = DES(\overline{K}, M) = Y = DES(T, M)$. Logo $K = \overline{T}$

Portanto verifica-se ao mesmo tempo duas possibilidades para K: T e $\overline{T}$. Logo o número de tentativas é reduzido pela metade.

Uma maneira de se evitar esta fraqueza é não enviar mensagens complementares e evitar o uso de chaves complementares.

1.3.2 Existência de Chaves Fracas

Após a aplicação da Permutação Escolha 1 à chave de ciframento, o resultado é dividido em duas metades C e D. Se C e D forem compostos apenas de 0's ou 1's então as subchaves utilizadas durante o processo de ciframento serão todas idênticas pois os deslocamentos circulares à esquerda determinarão sempre os mesmos valores para C e D ao longo do processo de geração das subchaves. Chaves de ciframento para as quais este fenômeno ocorre são denominadas **chaves fracas**. Para estas chaves o processo de ciframento é o mesmo que o de deciframento: sejam M uma mensagem, K uma chave fraca e C o criptograma obtido cifrando-se M com K. C = DES(K,M) e M = DES(K,C). Note que não é necessário utilizar o processo de deciframento $DES^{-1}(K,C)$ para se obter M a partir de C.

As chaves fracas do DES estão representadas a seguir em forma hexadecimal:

Chave de Ciframento (64 bites)	Padrão Após Permutação Escolha 1 (56 bites)
01 01 01 01 01 01 01 01	00 00 00 00 00 00 00
FE FE FE FE FE FE FE FE	11 11 11 11 11 11 11
1F 1F 1F 1F 0E 0E 0E 0E	00 00 00 01 11 11 11
E0 E0 E0 E0 F1 F1 F1 F1	11 11 11 10 00 00 00

Tabela 1.3.2a: Chaves Fracas do DES

Como o número de chaves fracas é pequeno é perfeitamente possível evitá-las.

1.3.3 Existência de Chaves Semi-Fracas

Existem pares de chaves distintas de ciframento K_1 e K_2 tais que se $C = DES(K_1,M)$ então $M = DES(K_2,C)$, ou seja, $C = DES^{-1}(K_2,M)$. Isto significa que K_1 pode decifrar uma mensagem cifrada com K_2 e vice-versa. Estas chaves são denominadas **chaves semi-fracas** e são representadas abaixo na forma hexadecimal.

01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E0 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

Tabela 1.3.3a: Pares de Chaves Semi-Fracas

1.3.4 Colisão de Chaves

Denomina-se **colisão de chaves** o fato de duas chaves distintas gerarem o mesmo criptograma a partir da mesma mensagem. Outras chaves com esta característica, além das Chaves Semi-Fracas apresentadas anteriormente, foram pesquisadas por [DQ84] e algumas foram determinadas para aplicações do DES com 1, 2 ou 3 iterações.

[QD89] apresenta algumas colisões de chaves para determinadas mensagens utilizando o DES com 16 iterações. Por exemplo, a mensagem, em notação hexadecimal, 0404040404040404 cifrada com a chave 46b2c8b62818f884 ou com a chave 4a5aa8d0ba30585a, apresenta o mesmo criptograma: f02d67223ceaf91c.

Capítulo 2

Visão Geral de Criptoanálise

2.1 Conceitos Fundamentais

Quebrar um criptograma significa descobrir a mensagem a partir da qual ele foi obtido. **Quebrar uma chave** significa obter a chave utilizada no ciframento de uma mensagem. Um sistema criptográfico é quebrado se é possível determinar a mensagem ou a chave utilizada no ciframento a partir do criptograma ou pares mensagem-criptograma.

Atacar um sistema criptográfico significa tentar quebrar um criptograma ou uma chave.

Um sistema criptográfico é **incondicionalmente seguro** se não é possível obter-se informações nos criptogramas interceptados que permitam determinar de maneira única a mensagem ou a chave.

Robustez de um sistema criptográfico é o tempo necessário para quebrar uma chave.

Um sistema criptográfico é **computacionalmente seguro** ou **forte** se o tempo necessário para quebrá-lo é computacionalmente inviável.

Criptoanálise é a ciência que estuda métodos para quebrar sistemas criptográficos.

As seguintes hipóteses devem ser feitas pelo projetista de um sistema criptográfico: o algoritmo de ciframento é conhecido pelo criptoanalista e este pode ter acesso aos criptogramas através de algum método de escuta.

2.2 Métodos Básicos de Criptoanálise para Sistemas Simétricos

Existem três métodos básicos de criptoanálise para sistemas simétricos que definiremos a seguir: criptograma conhecido ("ciphertext-only attack"), mensagem conhecida ("known-plaintext attack") e mensagem escolhida ("chosen-plaintext attack") [D82].

No método de criptograma conhecido o criptoanalista deve determinar a chave examinando apenas a mensagem ou apenas o criptograma. Neste caso a quebra se baseia em probabilidades, distribuições e características dos criptogramas disponíveis [D82].

No método de mensagem conhecida o criptoanalista tem acesso a pares correspondentes (mensagem,criptograma). Neste caso o criptoanalista tem conhecimento sobre a mensagem ou partes desta. Isto pode ocorrer, por exemplo, quando todas as mensagens enviadas possuem uma mesma seqüência de caracteres em alguma parte de seu conteúdo (identificação do terminal, nome da empresa, etc.) [D82].

No método de mensagem escolhida o criptoanalista pode escolher a mensagem a ser cifrada. Isto pode ocorrer de duas formas: o criptoanalista consegue induzir a transmissão de uma mensagem ou o criptoanalista tem acesso ao dispositivo de ciframento, mesmo não conhecendo a chave [D82]. Esta última hipótese é muito forte pois o criptoanalista deve ter a possibilidade de injetar no dispositivo de ciframento várias mensagens escolhidas por ele, o que torna este ataque muito difícil de ocorrer na prática. Apesar disto, é uma criptoanálise que permite comparar a robustez de dois criptossistemas distintos.

2.3 Cadeias de Markov e Processos Markovianos: uma introdução [F50]

2.3.1 Cadeias de Markov

Para uma seqüência de experimentos independentes com possíveis resultados E_1, E_2,..., onde cada resultado possui uma probabilidade associada p_k, a probabilidade de uma seqüência de resultados ocorrer é igual ao produto das probabilidades associadas a cada

resultado da seqüência. Por exemplo, jogando-se simultaneamente uma moeda e um dado, a probabilidade de dar cara e o número 5 é $\frac{1}{2} \times \frac{1}{6}$.

Na teoria de cadeias de Markov, o resultado de qualquer experimento depende *apenas* do resultado do experimento imediatamente anterior. Um resultado E_k não possui uma probabilidade fixa associada p_k , porém para todo par de resultados (E_j,E_k), indicando que E_j ocorreu imediatamente antes de E_k, existe uma probabilidade fixa condicional p_{jk}, também denotada por $P(E_k \mid E_j)$, que é a probabilidade de E_k ocorrer dado que E_j ocorreu anteriormente. E_k também possui uma probabilidade associada a_k, que é a probabilidade de E_k ser o resultado inicial de uma seqüência de experimentos.

Portanto, dada uma seqüência de experimentos, a probabilidade de uma seqüência de resultados $(E_{r0}, E_{r1}, ..., E_{rn})$, onde o primeiro resultado da seqüência possui índice r0, o segundo índice r1 e assim sucessivamente, ocorrer é igual a

(2.1) $$a_{r0} \cdot p_{r0r1} \cdot p_{r1r2} \cdots p_{r(n-2)r(n-1)} \cdot p_{r(n-1)rn} \cdot$$

Esta probabilidade também é denominada probabilidade composta de $(E_{r0}, E_{r1}, ..., E_{rn})$

Qualquer seqüência de experimentos é uma **cadeia de Markov** se a probabilidade de ocorrência de qualquer seqüência de resultados é dada pela expressão acima, em termos de uma distribuição de probabilidades iniciais $\{a_k\}$ para os resultados E_k e probabilidades fixas condicionais p_{jk} de E_k, dado que E_j ocorreu no experimento anterior.

Mudando-se a notação para que esta seja mais adequada às aplicações físicas, ao invés de dizermos "o resultado do experimento *n* é E_k" diremos "o estado do sistema no instante *n* é E_k". A probabilidade condicional p_{jk} será denominada probabilidade de transição do estado E_j para o estado E_k e denotada por $E_j \rightarrow E_k$.

Uma cadeia de Markov é chamada **homogênea** quando $P(E_{i+1}=\beta \mid E_i=\alpha)$ é independente de i para todo α e β [LM91]. Fisicamente isto significa que as probabilidades de transição independem do tempo [So87].

Seja p_i a probabilidade do estado inicial ser i, para todo i pertencente ao conjunto S de estados do sistema. O **vetor de probabilidades iniciais** $p = (p_0, p_1, p_2, ...)$ sobre S satisfaz as seguintes propriedades [So87]:

1. $0 \leq p_i \leq 1$, para todo $i \in S$.
2. $\sum_{i \in S} p_i = 1$, pois o processo deve começar em algum lugar no instante 0.

O **vetor de probabilidades no instante** t é definido como $p^t = (p^t_0, p^t_1, p^t_2, ..., p^t_N)$, onde $p^t_j = P(E_t = j|$ vetor inicial p), isto é, a probabilidade do sistema estar no estado j dado que o estado inicial tem probabilidades dadas pelo vetor de probabilidades iniciais p.

Um **vetor de probabilidades** $\rho = (\rho_0, \rho_1, \rho_2, ...)$ satisfaz as seguintes propriedades [So87]:

1. $0 \leq \rho_i \leq 1$, para cada $i \in \{0, 1, 2, ..., N\}$.
2. $\rho_0 + \rho_1 + ... + \rho_N = 1$.

Suponha que existam n partículas que podem saltar de um estado para outro de acordo com uma distribuição de probabilidades de transição. Se todas as partículas estão no estado 0 no instante t = 0 então o número de partículas que podem estar no estado j após a primeira transição é $n.p_{0j}$. Suponha que as n partículas são distribuídas de maneira que n_j partículas estão no estado j no instante t = 0, para j = 0, 1, ..., N. O número de partículas em cada estado j que podem estar no estado i após uma transição é $n_j.p_{ji}$. O número total de partículas que podem estar no estado i após uma transição é

$$n_i = \sum_{j=0}^{N} n_j \cdot p_{ji} \tag{2.2}$$

Pode acontecer que o número de partículas no estado i seja idêntico ao número de partículas neste estado no instante inicial. As partículas realizam transições porém o número total de partículas não se altera, pois cada partícula que deixa o estado i é substituída por outra que faz uma transição para este. Se isto ocorrer para todos os estados dizemos que o sistema de n partículas está em um **estado de equiliíbrio** [So87].

Podemos reescrever a equação (2.2) em termos do número relativo de partículas no estado i, ou seja a probabilidade de uma partícula ocupar o estado i.

(2.3) $$\pi(\mathrm{i}) = \frac{n_i}{n} = \sum_{j=0}^{N} \frac{n_j}{n} \cdot p_{ji}$$

Se a equação (2.3) vale para todos os estados então o sistema está em estado de equilíbrio. Um vetor de probabilidades ϕ representa um estado de equilíbrio se $\phi_i = \sum_{j=0}^{N} \phi j \, . \, p_{ji}$ [So87].

O estado de equilíbrio corresponde à estabilidade do sistema após um número muito grande de transições [Ka79], isto é, $P(E_t = i|$ vetor inicial p) $\rightarrow \phi_i$, a medida que $t \rightarrow \infty$ para cada estado i do conjunto S de estados , não importando o vetor de probabilidades iniciais p, isto é as probabilidades de transição são dadas pelo vetor $\phi = (\phi_1, \phi_2, ...)$ [So87].

Se $\pi(i) \geq 0$ para todo i ε S, $\sum_{x \varepsilon S} \pi(x) = 1$ e satisfaz a equação (2.3) então a distribuição de probabilidades $\{ \pi(x), x \varepsilon S \}$ é chamada **distribuição estacionária** [Ka79].

Uma cadeia de Markov é estacionária se a distribuição de probabilidades de transição é estacionária., isto é, todas as transições de estado têm a mesma distribuição de probabibilades.

2.3.2 Processos Markovianos

Em algumas aplicações é conveniente descrever cadeias de Markov em termos de variáveis aleatórias. Neste caso denotaremos o estado E_k por um inteiro k. O estado do sistema no instante n é uma variável aleatória $X^{(n)}$, que assume um valor k com probabilidade $a_k^{(n)}$. A probabilidade composta de $X^{(n)}$ e $X^{(n+1)}$ é igual à probabilidade de que $\{ X^{(n)} = j, X^{(n+1)} = k \} = a_j^{(n)} p_{jk}$, e a probabilidade composta de $(X^{(0)},..., X^{(n)})$ ocorrer é dada por (2.1). Utilizando-se esta notação, uma cadeia de Markov se transforma em um processo estocástico (também chamado processo aleatório), isto é, uma seqüência de variáveis aleatórias $(X^{(0)},..., X^{(n)})$, em que cada subconjunto finito desta possui uma distribuição de probabilidades compostas bem definidas.

Processos Markovianos são uma classe de processos estocásticos. Em processos estocásticos o estado futuro não é determinado de maneira única, porém existem probabilidades relacionando o estado presente com o futuro que permitem uma previsão. Em processos Markovianos o estado futuro depende apenas do estado atual não importando como se chegou a este estado., isto é, dado um sistema em uma estado s_i em um instante n_i, nenhuma informação adicional a respeito dos estados do sistema nos instantes anteriores pode alterar as probabilidades condicionais de um estado s em um instante futuro n: em um processo Markoviano se dois sistemas independentes com probabilidades de transição idênticas evoluem para um mesmo estado em um mesmo instante então todas as probabilidades relacionadas aos seus estados futuros são idênticas não importando como estes sistemas chegaram ao estado atual.

Processos mecânicos que "não guardam memória de seu passado", isto é, o estado futuro depende apenas do estado presente são exemplos de processos Markovianos. Um exemplo seria uma partícula com movimento aleatório. Neste caso a próxima posição da partícula depende apenas da posição atual. Um exemplo de processo mecânico que não é Markoviano é o processo de deformação plástica. Neste caso o estado futuro depende dos estados passados.

2.4 Criptossistemas Iterativos e Criptoanálise Diferencial

2.4.1 Introdução

Criptossistemas Iterativos são uma família de sistemas criptográficos fortes que consistem em iterar n vezes uma função criptograficamente fraca (o sistema é dito de n-iterações). Neste trabalho esta função será denominada **função de iteração**.

A **Criptoanálise Diferencial** é um método de criptoanálise do tipo mensagem escolhida aplicável a criptossistemas iterativos [BS90, BS91, Kn92]. O método consiste em analisar o efeito de diferenças particulares em pares de mensagens nos respectivos pares de criptogramas. O método é aplicado em muitos pares de mensagens, todos com a mesma diferença particular. Estas diferenças podem ser utilizadas para associar probabilidades a possíveis chaves, para determinar a chave mais provável. Para os sistemas semelhantes ao

DES, a diferença particular é um valor fixo correspondente ao XOR entre as mensagens de cada par [BS91].

Uma função criptográfica $F(R,K_i)$, onde R é uma mensagem e K_i uma subchave, é **criptograficamente fraca** se com algumas triplas (R',Y,Y*)., onde R' é a diferença entre um par de mensagens (R,R*), Y e Y* são respectivamente os resultados de $F(R,K_i)$ e $F(R^*,K_i)$, é possível determinar K_i [LM91].

Vamos agora introduzir a seguinte notação:

n_X: é um número hexadecimal (e.g., $1A_X = 26$)

X, X* e X': X e X* são os resultados intermediários do processo de ciframento de cada elemento de um par de mensagens. X' é a diferença entre X e X* (para o DES, $X' = X \oplus X^*$, onde $\oplus$ é o símbolo de XOR).

P(X): A permutação P é denotada por P(X). A letra P sozinha representa uma mensagem .

E(X): Expansão E.

IP(X): Permutação Inicial[1].

P: Uma mensagem (após a aplicação da Permutação Inicial). P* é a outra mensagem de um par de ciframentos. P' é a diferença entre P e P* (para o DES, $P' = P \oplus P^*$, onde $\oplus$ é o símbolo de XOR).

T: Os criptogramas correspondentes às mensagens P e P* (antes da aplicação da Inversa da Permutação Inicial) são denotados por T e T*. T' é a diferença entre T e T* (para o DES, $T' = T \oplus T^*$, onde $\oplus$ é o símbolo de XOR). Quando o número de iterações executadas for relevante denotaremos o criptograma obtido após i iterações por T(i). Se o processo de ciframento é composto de n iterações então T(n)=T.

---

[1] Neste trabalho a Permutação Inicial (IP) e a sua inversa (IP^{-1}) serão ignoradas pois elas são irrelevantes para a criptoanálise diferencial [BS91].

(L,R): As metades esquerda e direita de uma mensagem P são denotadas respectivamente por L e R.

(*l*,*r*): As metades esquerda e direita de um criptograma T são denotadas respectivamente por *l* e *r*.

a, *b*, *c*, ..., *j*,...,*p*: Cada entrada de 32 bits da função F em cada iteração do DES.

A, B, C, ..., J,...,P: Cada saída de 32 bits da função F em cada iteração do DES.

S_i: São as Caixas de Substituição (S-boxes) S_1, S_2, ...,S_{16}.

S_i^{EX}, S_i^{KX}, S_i^{IX}, S_i^{OX}: A entrada de cada Caixa de Substituição na iteração X é denotada por S_i^{IX} para X ε {a,...,j}. A saída de cada Caixa de Substituição na iteração X é denotada por S_i^{OX}. Cada subconjunto de 6 bits da subchave que é entrada na Caixa de Substituição S_i é denotado por S_i^{KX} e cada subconjunto de 6 bits da saída da expansão E(X) é denotado por S_i^{EX} (vide Figura 2.4.1b).

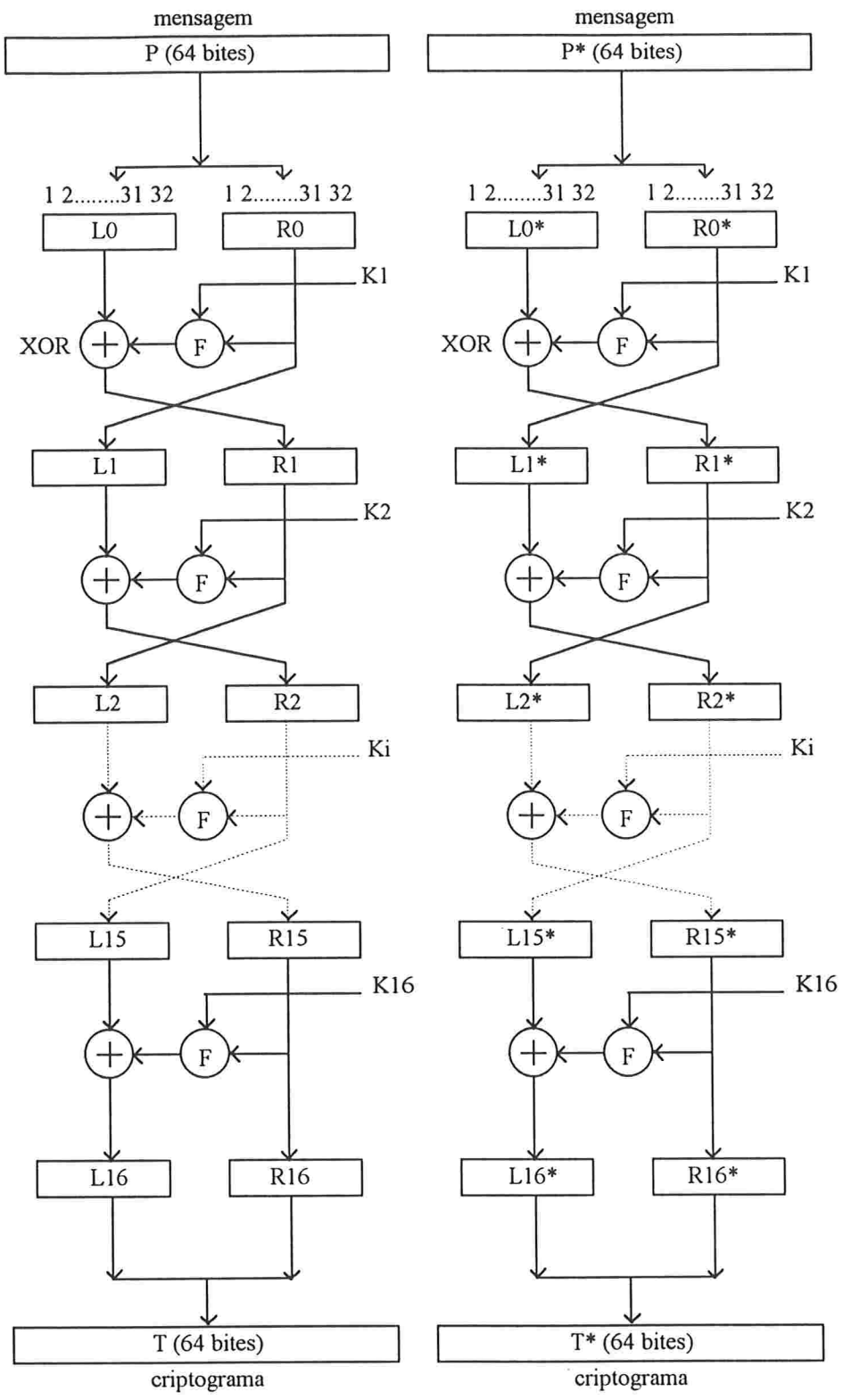


Figura 2.4.1a: Ilustração do ciframento de um par de mensagens

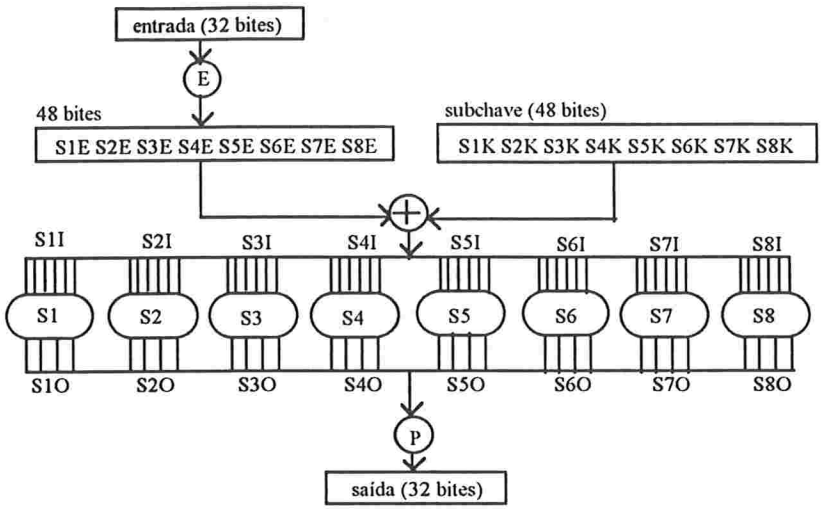


Figura 2.4.1b: Função F

2.4.2 Algumas Características da Função de Ciframento F do DES

Fixemos uma subchave K_i e um par de mensagens com XOR conhecido. Os seguintes resultados seguem da maneira como a função F foi projetada [BS91]:

1) o XOR entre as saídas da expansão E é calculado da seguinte forma:
$E(X) \oplus E(X^*) = E(X \oplus X^*)$.

2) o valor do XOR na saída da expansão E continua válido após o XOR com a subchave:
$(X \oplus K_i) \oplus (X^* \oplus K_i) = X \oplus X^*$.

3) o valor do XOR entre os componentes do par de criptogramas antes da aplicação da permutação P continua válido após sua aplicação:
$P(X) \oplus P(X^*) = P(X \oplus X^*)$.

4) as Caixas de Substituição não são lineares. Logo o conhecimento do XOR entre um par de entradas numa Caixa de Substituição não garante que se conheça o XOR entre o par correspondente às saídas (um caso especial ocorre quando as entradas são idênticas, neste caso as saídas também o são). As Caixas de Substituição possuem algumas características de projeto que são conhecidas:

4.1. Nenhuma Caixa de Substituição é uma função linear ou afim.
4.2. Alterando um bit em uma entrada de uma Caixa de Substituição resulta em uma alteração de no mínimo dois bites na saída.
4.3. S(X) e S(X $\oplus$ 001100) diferem em no mínimo dois bites.
4.4. S(X) $\neq$ S(X $\oplus$ 11xy00) para quaisquer x e y.
4.5. As Caixas de Substituição foram projetadas de forma a minimizar as diferenças entre o número de 1's e 0's em qualquer saída de uma Caixa de Substituição quando algum bit da entrada é mantido constante.

2.4.3 Criptoanálise Diferencial de Criptossistemas Iterativos

Uma **chave independente*** é uma lista de n subchaves que não derivam necessariamente da mesma chave através do esquema de geração de subchaves [BS91].

> O DES possui $2^{16.48=768}$ possíveis chaves independentes (16 subchaves, cada uma com 48 bites) mas apenas 2^{56} chaves possíveis.

Associado a qualquer par de ciframentos há o seguinte conjunto denominado **característica** ou **característica de n-iterações** composto dos seguintes valores: diferença entre as mensagens (denotado por P'), diferença entre as saídas de cada iteração do processo de ciframento e diferença entre os criptogramas (denotado por T'). Uma característica tem uma probabilidade associada que é a probabilidade de que um par aleatório de mensagens com um P' escolhido tenha os mesmos valores de diferença especificados na característica [BS91].

Um **diferencial de n-iterações** é uma dupla (α,β), onde α é a diferença de um par de mensagens distintas P e P*; e β é uma possível diferença entre os criptogramas T e T* após n iterações [LM91].

A **probabilidade de um diferencial de n-iterações** (α,β) ou **probabilidade diferencial** é a probabilidade condicional de que β é a diferença entre os criptogramas após n iterações dado que o par de mensagens tem diferença α quando P e as subchaves K_1, ...,

---

*Neste trabalho supõem-se que todas as chaves são independentes de modo a simplificar-se a análise probabilística do ataque [BS91].

K_n são independentes e uniformemente aleatórias. Esta probabilidade é denotada por $P(T' = \beta|P' = \alpha)$ [LM91].

Uma característica de n-iterações é uma (n+1)-upla $(\alpha,\beta_1, ...,\beta_n)$ considerada como um possível valor para (P', T'(1), ..., T'(n)). Uma característica de 1-iteração coincide com um diferencial de 1-iteração e uma característica de n-iterações determina a sequência de n diferenciais, $(P',T'(_j)) = (\alpha,\beta_j)$. A probabilidade de uma característica de n-iterações pode então ser definida como $P(T'(1) = \beta_1, T'(2) = \beta_2, ..., T'(n) = \beta_n|P' = \alpha)$, quando P e as subchaves $K_1, ..., K_i$ são independentes e uniformemente aleatórias [LM91].

Lembrando que a criptoanálise diferencial é um método de criptoanálise do tipo mensagem escolhida, o procedimento básico de criptoanálise diferencial de um criptossistema iterativo de n-iterações é o seguinte [LM91]:

Algoritmo Quebra

(Passo 1) Achar um diferencial de (n-1) iterações (α,β) tal que $P(T'(n-1) = \beta|P' = \alpha)$ é máximo, ou próximo do máximo, através de um pré-cálculo de α's e β's escolhidos adequadamente. O processo de obtenção das probabilidades consiste em gerar vários pares de mensagens com diferença α e verificar a probabilidade com que os pares de criptogramas têm diferença β, supondo as subchaves independentes e uniformemente distribuídas. Repete-se o processo para vários α's e β's. Para a utilização destas probabilidades calculadas assume-se a hipótese EE, apresentada no item 2.4.4.

(Passo 2) Escolher aleatoriamente uma mensagem P (com distribuição uniforme) e calcular P* tal que $P' = \alpha$. Cifrar P e P* com a chave K que se deseja quebrar.

Se $T'(n-1)= \beta$ então vá para o passo (3) senão volte para o passo (2).

(Passo 3) A partir de T(n) e T*(n) determinar todos os possíveis valores para a subchave K_n (utilizada na última iteração) que correspondam a diferença $T'(n-1) = \beta$ (obtida na saída da iteração anterior). Acrescentar uma unidade ao contador de cada possível valor determinado para K_n.

(Passo 4) Repita os passo (2) e (3) até que um ou mais valores possíveis para K_n ocorram com maior freqüência em relação aos outros. Deve-se então selecionar os valores mais freqüentes como candidatos a verdadeira subchave K_n.

Note que o algoritmo Quebra permite determinar a subchave K_n, portanto devemos repetir o algoritmo para as subchaves restantes. Por exemplo, para n=4, a seqüência de determinação das subchaves é K_4, K_3, K_2 e K_1. De posse das subchaves é possível obter a mensagem a partir do criptograma.

2.4.4 Cota Inferior para a Complexidade da Criptoanálise Diferencial

A cota inferior para complexidade da criptoanálise diferencial, denotada por Ω_d, é o número mínimo de ciframentos executados durante o ataque à uma subchave [BS91,LM91].

Em um ataque utilizando criptoanálise diferencial, todas as subchaves são fixas (o ataque é do tipo mensagem escolhida) e apenas o criptograma pode ser escolhido ao acaso. No cálculo de uma probabilidade diferencial, a mensagem e todas as subchaves são independentes e uniformemente aleatórias [LM91], conforme o suposto no Algoritmo de Quebra.

Antes de se iniciar o ataque, determina-se qual diferença utilizar a partir das probabilidades diferenciais previamente calculadas. A hipótese que é feita neste caso é a de *Equivalência Estocástica*:

Hipótese EE:

Para um diferencial de (n-1)-iterações (α,β),

$$P(T'(n-1) = \beta | P' = \alpha) \approx P(T'(n-1) = \beta | P' = \alpha, K_1 = \omega_1, ..., K_{n-1} = \omega_{n-1})^*,$$

para quase todos os valores possíveis de subchaves $(\omega_1, ..., \omega_{n-1})$ que levam um par de mensagens com diferença α a um par de criptogramas com diferença β [LM91].

Proposição 2.4.4: Um criptossistema é vulnerável a criptoanálise diferencial, ou seja, é possível quebrar uma subchave através do algoritmo Quebra, se e só se a função de iteração é criptograficamente fraca e existe um diferencial de (n-1)-iterações (α,β) tal que $P(T'(n-1) = \beta \mid P' = \alpha) >> \frac{1}{2^m}$, onde *m* é o comprimento de cada mensagem.

---

* Esta probabilidade não é constante para todas as subchaves porém é uma aproximação muito boa para a probabilidade diferencial [BS91,pág. 20].

Demonstração:

O número máximo de possíveis valores para a diferença T'(n-1) é 2^m - 1 pois cada mensagem tem comprimento m. A probabilidade de ocorrência aleatória de um valor para T'(n-1) é $\frac{1}{2^m - 1}$.

(⇐)

A função de iteração é criptograficamente fraca e existe um diferencial de (n-1)-iterações (α,β) tal que $P(T'(n-1) = \beta \mid P' = \alpha) >> \frac{1}{2^m}$. Portanto é possível achar um diferencial de (n-1) iterações (α,β) tal que $P(T'(n-1) = \beta|P' = \alpha)$ é máximo, ou próximo do máximo, pois $P(T'(n-1) = \beta|P' = \alpha)$ é muito maior do que a probabilidade de ocorrência aleatória de T'(n-1). Logo é possível atacar o criptossistema utilizando o algoritmo Quebra.

(⇒)

De acordo com a definição de criptoanálise diferencial, a função de iteração do criptossistema é criptograficamente fraca. Se o criptossistema pode ser atacado utilizando o algoritmo Quebra então existe um diferencial de (n-1) iterações (α,β) tal que $P(T'(n-1) = \beta| P' = \alpha)$ é máximo, ou próximo do máximo, isto é, $P(T'(n-1) = \beta|P' = \alpha)$ é bem maior do que a probabilidade de uma ocorrência aleatória de T'(n-1).Logo $P(T'(n-1) = \beta \mid P' = \alpha) >> \frac{1}{2^m}$.

◊

Teorema 2.4.4 Cota inferior para a criptoanálise diferencial de um criptossistema de n-iterações : Suponha que a hipótese EE é verdadeira, então em um ataque por criptoanálise diferencial, isto é, durante a determinação de uma subchave utilizando o algoritmo Quebra,

$\Omega_d \geq \frac{2}{p_{max} - \frac{1}{2^{m-1}}}$ onde $p_{max} = \max_{\alpha} \max_{\beta} P(T'(n-1) = \beta \mid P' = \alpha)^*$, m é o comprimento da mensagem e Ω_d definido no início do item 2.4.4. Em particular, se $p_{max} \approx \frac{1}{2^m - 1}$ então o ataque não terá sucesso.

---

* p_{max} é a maior probabilidade diferencial disponível

Demonstração:

A hipótese EE nos permite aplicar o algoritmo Quebra. p_{max} é a probabilidade de se obter um par de criptogramas com diferença β dado que o par de mensagens tem diferença α (note que para aplicarmos o algoritmo Quebra escolhemos um diferencial de modo que p_{max} seja o maior possível). Durante a execução do algoritmo Quebra, nem todos os pares de criptogramas podem ser aproveitados pois existe uma probabilidade de que a diferença do par não seja β, tendo-se então que escolher outro par de mensagens com diferença α.

Suponha que é possível quebrar uma subchave, utilizando o algoritmo Quebra, após N tentativas, onde cada tentativa consiste em escolher um par de mensagens com diferença α. Np_{max} é o número mínimo de tentativas em que se obteve um par de criptogramas com diferença β. Pela proposição 2.4.4, $p_{max} > \frac{1}{2^m - 1}$, ou seja, $Np_{max} > \frac{N}{2^m - 1}$ (multiplicando ambos os lados da expressão por N). Portanto $Np_{max} \geq \frac{N}{2^m - 1} + 1$ (removendo a desigualdade estrita). Logo $N \geq \frac{1}{p_{max} - \frac{1}{2^m - 1}}$. Como ocorrem N escolhas de pares de mensagens então 2N ciframentos são realizados. Concluimos então que $\Omega_d \geq \frac{2}{p_{max} - \frac{1}{2^m - 1}}$. Desta expressão observamos que se $p_{max} \approx \frac{1}{2^m - 1}$ então o ataque não terá sucesso.

◊

2.4.5 Criptossistemas de Markov

Um **grupo** consiste de [HK79]:

1) Um conjunto *C*;

2) Uma operação, denotada por $\otimes$, que associa a cada par de elementos (x,y) em *C* um elemento $x \otimes y$ em *C* com as seguintes propriedades:

(2.1) $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, para todo x, y , z ε *C*. Esta propriedade é denominada associatividade;

(2.2) existe um elemento $e \varepsilon C$ tal que $e \otimes x = x \otimes e = x$, para todo $x \varepsilon C$. *e* é chamado elemento neutro;

(2.3) a cada elemento x ε C corresponde um elemento x^{-1} ε C (denominado elemento inverso de x) tal que $x^{-1} \otimes x = x \otimes x^{-1} = e$.

Seja C um conjunto de mensagens (= conjunto de criptogramas). Um criptossistema iterativo com uma função de iteração $T=f(P,K_i)$ é um **criptossistema de Markov** ou **criptossistema markoviano** se existe uma operação de grupo ⊗ para definir diferenças entre elementos de C, tal que para qualquer α e β ($\alpha \neq e$ e $\beta \neq e$), $P(T' = \beta \mid P' = \alpha, P = \gamma)$ é independente de γ quando a subchave K_i é uniformemente aleatória, ou equivalentemente, se $P(T' = \beta \mid P' = \alpha, P = \gamma) = P(T' = \beta \mid P' = \alpha)$ para todas as escolhas de γ quando a subchave K_i é uniformemente aleatória [LM91].

Teorema 2.4.5.1 Se um criptossistema de n-iterações é markoviano e as n subchaves são independentes e uniformemente aleatórias, então a seqüência de diferenças P'=T'(0), T'(1), ..., T'(n) é uma cadeia de Markov homogênea. Além disso, esta cadeia é estacionária se P'é uniformemente distribuído sobre os elementos não neutros do grupo.

Demonstração:

Para mostrar que a seqüência P' , T'(1), ..., T'(n) é uma cadeia de Markov, é suficiente mostrar que para a segunda iteração

$$P(T'(2) = \beta_2 \mid T'(1) = \beta_1, P' = \alpha) = P(T'(2) = \beta_2 \mid T'(1) = \beta_1)$$

A parte esquerda pode ser reescrita como:

$$P(T'(2) = \beta_2 \mid T'(1) = \beta_1, P' = \alpha)$$
$$= \sum_{\gamma} [\, P(T(1) = \gamma,\ T'(2) = \beta_2 \mid T'(1) = \beta_1, P' = \alpha) \,]$$

A B C*

$$= \sum_{\gamma} [\, P(T(1) = \gamma \mid T'(1) = \beta_1, P' = \alpha) \cdot P(T'(2) = \beta_2 \mid T(1) = \gamma, T'(1) = \beta_1, P' = \alpha) \,]. \quad (a)$$

Como T(1) e T'(1) juntos determinam T(1) e T*(1) então T'(2) não depende mais de P' quando T(1) e T'(1) são especificados. Portanto podemos reescrever (a) como:

$$\sum_{\gamma} [\, P(T(1) = \gamma \mid T'(1) = \beta_1, P' = \alpha) \cdot P(T'(2) = \beta_2 \mid T'(1) = \beta_1, T(1) = \gamma) \,]. \quad (b)$$

---

* ordem de ocorrência dos eventos: C, A, B.

$$P(A, B|C) = \frac{P(A \cap B \cap C)}{P(C)} = \frac{P(C).P(A|C).P(B|A,C)}{P(C)} = P(A|C).P(B|A,C)$$

Como o criptossistema é markoviano então:
$P(T'(2) = \beta_2 \mid T'(1) = \beta_1, T(1) = \gamma) = P(T'(2) = \beta_2 \mid T'(1) = \beta_1)$

Podemos escrever (b) como:

$$\sum_{\gamma} [\, P(T(1) = \gamma \mid T'(1) = \beta_1, P' = \alpha) \cdot P(T'(2) = \beta_2 \mid T'(1) = \beta_1) \,]$$
$$= P(T'(2) = \beta_2 \mid T'(1) = \beta_1) \cdot \sum_{\gamma} P(T(1) = \gamma \mid T'(1) = \beta_1, P' = \alpha)$$
$$= P(T'(2) = \beta_2 \mid T'(1) = \beta_1) \cdot 1$$
$$= P(T'(2) = \beta_2 \mid T'(1) = \beta_1).$$

Como em cada iteração utiliza-se a mesma função de iteração então P'=T'(0), T'(1), ..., T'(n) é uma cadeia de Markov homogênea.

Para cada chave K = k, a função de iteração f(•,k) é uma função pseudo-aleatória, no sentido de que não é injetora com baixa probabilidade (característica desejável do ponto de vista de projeto). Portanto a função f leva pares de mensagens distintas (P,P*) em pares de criptogramas distintos (T = F(P,k),T* = F(P*,k)) com alta probabilidade. Como P e P' ($\neq e$) são independentes e uniformemente distribuídos então (P,P*) é uniformemente distribuído sobre os pares distintos de mensagens. Portanto (T,T*) também é uniformemente distribuído sobre os pares distintos de criptogramas e então T' ($\neq e$) é também uniformemente distribuído. Portanto a distribuição uniforme é uma distribuição estacionária para esta cadeia de Markov pois todas os valores para as diferenças T' possuem a mesma probabilidade (vide item 2.3.1 para a definição de distribuição estacionária).
◊

Para um criptossistema markoviano com subchaves independentes e uniformemente aleatórias, a probabilidade para uma característica de n-iterações é dada pela equação de Chapman-Kolmogorov para uma cadeia de Markov [F50,Ka79,LM91,So87]:

$$P(T'(1) = \beta^*_1, T'(2) = \beta^*_2, \ldots, T'(n) = \beta^*_n \mid T'(0) = P' = \beta^*_0) = \prod_{i=1}^{n} P(T'(i) = \beta^*_i \mid T'(i-1) = \beta^*_{i-1})$$

Portanto a probabilidade de um diferencial de n-iterações (β_0, β_n) é

$$P(T'(n) = \beta_n \mid T'(0) = P' = \beta_0) = \sum_{\beta_1} \sum_{\beta_2} \cdots \sum_{\beta_{n-1}} \prod_{i=1}^{n} P(T'(i) = \beta_i \mid T'(i-1) = \beta_{i-1})$$

onde as somatórias são sobre todos os possíveis valores para diferenças β_i entre elementos distintos, isto é, sobre todos os elementos do grupo com exceção do elemento neutro [LM91].

Proposição 2.4.5: O DES é um criptossistema markoviano para uma definição de diferença $P' = P \oplus P^*$, supondo subchaves independentes e uniformemente aleatórias.

Demonstração:

Seja C o conjunto de mensagens. Verifica-se:

1. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, $\forall$ x, y e z ε C.
2. Seja $e = 0 \varepsilon C$. $x \oplus 0 = 0 \oplus x = x$, $\forall$ x ε C.
3. Seja $x^{-1} = x$. $x \oplus x^{-1} = x^{-1} \oplus x = 0$, $\forall$ x ε C.

Logo $\oplus$ é uma operação de grupo.

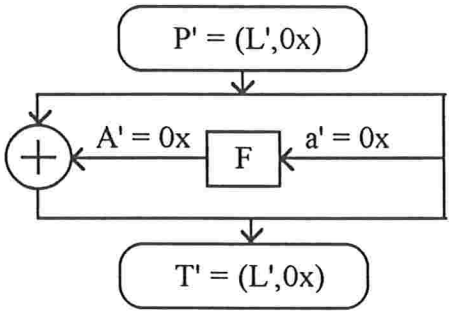
Pelo Lema 1 de [BS91], no DES a probabilidade de um diferencial (α,β) é igual a fração de subchaves possíveis que levam um par de mensagens com diferença α a um par de criptogramas com diferença β. Portanto $P(T' = \beta \mid P' = \alpha, P = \gamma)$ é independente de γ quando as subchaves são independentes e uniformemente aleatórias. Pelo fato de que $\oplus$ é uma operação de grupo e como $P(T' = \beta \mid P' = \alpha, P = \gamma)$ é independente de γ quando as subchaves são independentes e uniformemente aleatórias, conclui-se que o DES é um criptossistema markoviano.

$\Diamond$

2.4.6 Exemplos de Características

Apresentamos a seguir algumas características para o DES [BS91].

2.4.6.1 Característica de 1-iteração com probabilidade 1

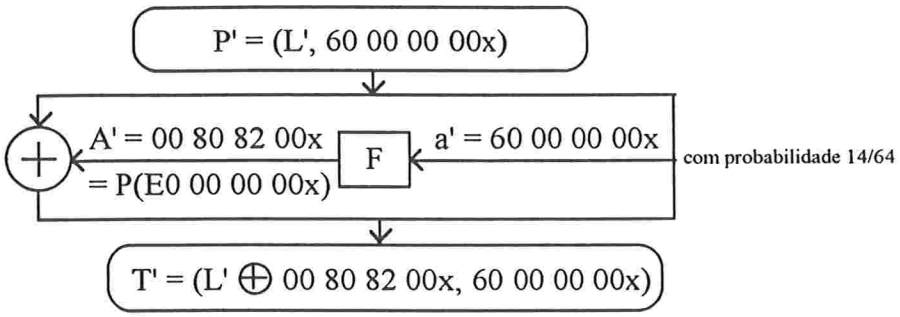


Não importa qual seja o valor de L', o XOR entre as saídas é $(L',0_X)$ com probabilidade 1, pois o XOR entre o par de entrada em F é zero (os elementos do par são idênticos).

2.4.6.2 Característica de 1-iteração com probabilidade 14/64

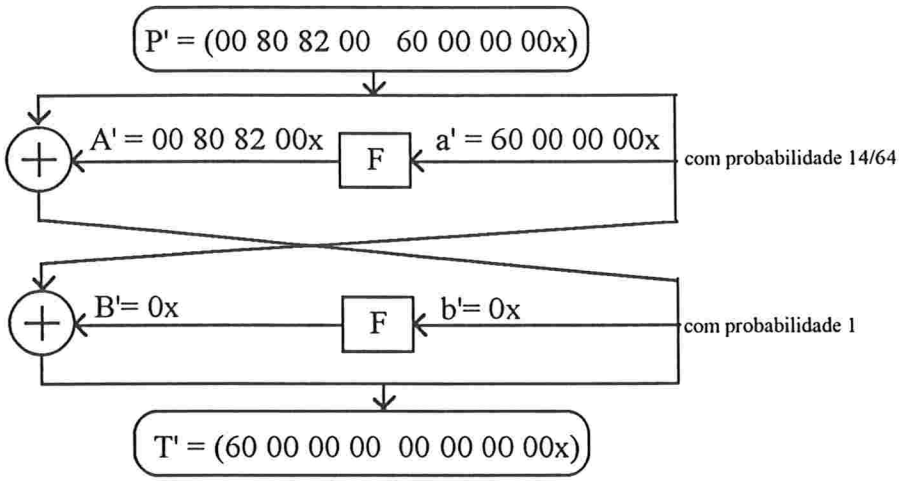
De acordo com a Tabela 27 em [pág 64, BS91], um par de entradas em S1 com XOR igual a $0C_X$ leva a um XOR de saída de valor E_X com probabilidade 14/64. Um XOR de entrada igual a zero em qualquer Caixa de Substituição (S-Box) Si leva a um XOR de saída de valor zero.

Seja P'= (L', 60 00 00 00_X). Conforme o item 2.4.2, S'^{I1} = E(60 00 00 00_X) = 30 00 00 00 00 00_X. Logo $S'_1{}^{I1} = 001100_b = 0C_X$, e $S'_2{}^{I1} = S'_3{}^{I1} = S'_4{}^{I1} = S'_5{}^{I1} = S'_6{}^{I1} = S'_7{}^{I1} = S'_8{}^{I1} = 0$. Portanto $S'_1{}^{O1} = E_X$ e S'^{O1} = E0 00 00 00_X com probabilidade 14/64. Então de acordo com o item 2.4.2, A' = P(E0 00 00 00_X) = 00 80 82 00_X (vide figura abaixo).



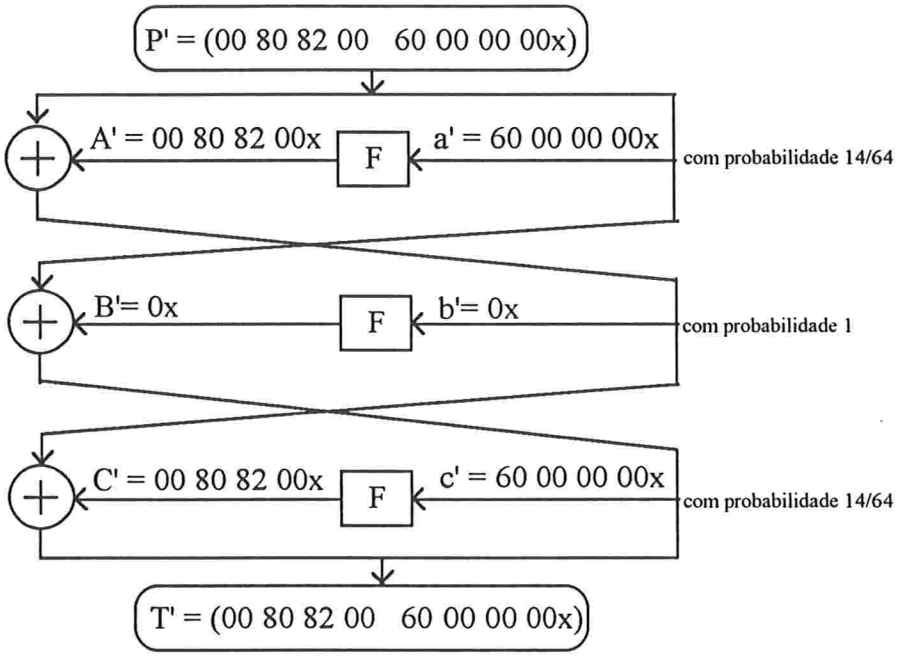
2.4.6.3 Característica de 2-iterações com probabilidade 14/64

A característica abaixo é obtida concatenando-se as duas características anteriores:



2.4.6.4 Característica de 3-iterações com probabilidade $(14/64)^2$

A característica a seguir é obtida concatenando-se os dois exemplos iniciais de uma maneira particular.



Note a utilização da característica de probabilidade 1 na segunda iteração e a simetria apresentada. A concatenação das duas características, permite obter uma característica maior com uma probabilidade aproximadamente* igual ao produto das suas probabilidades. A vantagem de se utilizar características com a simetria apresentada é a de obter-se características longas, com uma redução de probabilidade muito pequena.

As características com as quais é possível fazer-se concatenações onde a redução de probabilidade é muito pequena são chamadas **iterativas** [BS90,BS91].

---

* hipótese EE

Capítulo 3

Proposta de Fortalecimento do DES contra Criptoanálise Diferencial

3.1 Resultados Obtidos por Biham e Shamir

Os resultados obtidos por Biham e Shamir no ataque ao DES, utilizando criptoanálise diferencial, são os seguintes [BS92]:

No. de Iterações	Complexidade do Ataque
8	2^{14}
9	2^{24}
10	2^{24}
11	2^{31}
12	2^{31}
13	2^{39}
14	2^{39}
15	2^{47}
16	2^{47}

Tabela 3.1: Criptoanálise do DES

Verifica-se na tabela acima que a complexidade para um ataque ao DES com 16 iterações é inferior à complexidade de um ataque por busca exaustiva (vide item 1.3.1).

As seguintes possíveis modificações no algoritmo do DES foram analisadas por Biham e Shamir e os resultados são os seguintes [BS91]:

(1) Modificação no esquema de geração de subchaves não fortalecem o DES. A utilização de subchaves independentes também não modifica esta situação.

(2) Ataques contra o DES com número de iterações variando entre 9 e 16 não são influenciados pela permutação P. Portanto a substituição desta permutação por outra não fortalecerá o criptossistema.

(3) A mudança na ordem das Caixas de Substituição (S-Boxes) pode tornar o DES mais vulnerável à criptoanálise diferencial.

(4) A substituição da operação XOR por outra pode tornar o DES mais fraco.

(5) O DES com Caixas de Substituição aleatórias é fácil de quebrar.

Em seu ataque ao DES com 16 iterações Biham e Shamir utilizam a seguinte característica iterativa:

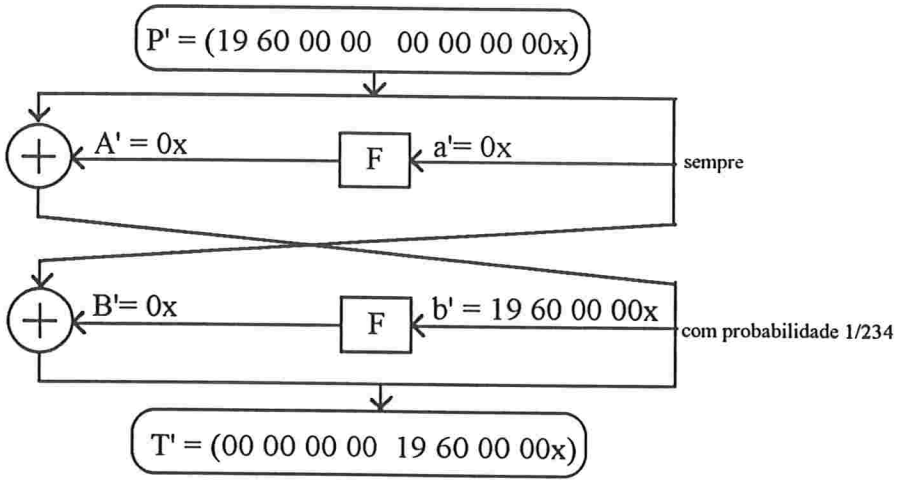


Figura 3.1a: Característica utilizada por Biham e Shamir em seu ataque ao DES

Biham e Shamir constroem uma característica de 13 iterações, com probabilidade aproximadamente igual a $2^{-47.2}$, iterando 6,5 vezes a característica anterior, para quebrar o DES com 16 iterações. O ataque que Biham e Shamir realizam é diferente do algoritmo de Quebra apresentado no item 2.4.3, pois eles não constroem uma característica de 16 iterações para determinar K16, uma de 15 iterações para determinar K15 e assim sucessivamente. Biham e Shamir utilizam uma característica de 13 iterações junto com outras técnicas (entre elas, inspeção das saídas nas caixas de substituição, estimativa de bites da chave a partir das subchaves mais prováveis) para determinar diretamente os bites da chave de ciframento.

Note que no algoritmo Quebra determinamos as subchaves e não a chave de ciframento.

Segundo [Kn92], Biham e Shamir utilizam em seu ataque ao DES características iterativas que podem ser as melhores características que se consegue encontrar para o DES.

3.2 Alguns Estudos Realizados em Criptossistemas Iterativos

Criptossistema LOKI

O LOKI é um criptossistema simétrico, de mensagens de 64 bites em criptogramas de 64 bites, utilizando uma chave de ciframento de 64 bites, proposto por Brown, Pieprzyk e Seberry em [BPS90], com uma estrutura semelhante ao DES, no sentido de que possui um esquema de geração de subchaves, expansões, permutações e caixas de substituição (S-boxes). As principais diferenças entre o LOKI e o DES são:
(i) o LOKI possui quatro caixas de substituição, onde cada uma tem uma entrada de 12 bites e uma saída de 8 bites. A saída é calculada através de exponenciações.
(ii) no LOKI faz-se um XOR entre a chave de ciframento e a mensagem antes da primeira iteração e um XOR entre a chave de ciframento e o criptograma após a última das 16 iterações.

Foi apresentada em [Kn91] a criptoanálise diferencial do LOKI, monstrando-se então que este criptossistema é vulnerável a este tipo de ataque, com uma complexidade menor do que um ataque por busca exaustiva (vide item 1.3.1).

Algumas modificações foram propostas ao LOKI em [BKPS91] para fortalecê-lo contra a criptoanálise diferencial. As alterações efetuadas no algoritmo foram as seguintes:
1. Alteração do esquema de geração de subchaves.
2. Remoção dos XOR's realizados entre a chave com a mensagem e com o criptograma
3. Alteração das caixas de substituição.

Em [BKPS91] é mostrado que para o novo LOKI, com 16 iterações, a criptoanálise diferencial torna-se quase impossível.

Criptossistema PES

O PES é um criptossistema simétrico, de mensagens de 64 bites em criptogramas de 64 bites, utilizando uma chave de ciframento de 64 bites, proposto por Lai e Massey em [LM90]. Este algoritmo de ciframento é baseado em três operações sobre blocos de 16 bites: XOR, adição módulo 2^{16} e multiplicação módulo $2^{16}+1$. A mensagem e a chave são divididos em quatro blocos de 16 bites e cada iteração do algoritmo consiste em realizar as operações anteriores entre blocos de entrada e blocos de chave, obtendo-se blocos intermediários, e então realizar estas mesmas operações com os blocos intermediários, entre si ou entre blocos de chaves, várias vezes, em uma ordem preestabelecida. Por fim realiza-se uma permutação dos blocos obtidos.

Em [LM91] Lai e Massey apresentam a criptoanálise diferencial do PES e sugerem uma modificação no algoritmo, que consiste em uma pequena alteração no esquema de permutações de blocos. Com esta modificação, Lai e Massey demonstram em [LM91] que o novo PES possui uma resistência bem alta à criptoanálise diferencial.

Criptossistema RDES

O criptossistema RDES, apresentado por Koyama e Terada em [KT93], consiste basicamente no algoritmo DES com uma pequena modificação: as trocas sistemáticas Sw são substituídas por trocas probabilísticas, que só ocorrem se um determinado bit da chave for igual a 1. Foi demonstrado em [KT93] que a robustez do RDES com 16 iterações, contra um ataque por criptoanálise diferencial, é equivalente à robustez do DES com 20 iterações.

3.3 Proposta de Alteração do DES

3.3.1 Finalidade

Uma maneira de aumentar a resistência do DES com 16 iterações à criptoanálise diferencial é diminuir as probabilidades diferenciais associadas às características utilizadas por Biham-Shamir no seu ataque. A nossa proposta consiste em alterar o algoritmo do DES, introduzindo um componente probabilístico que não altere as propriedades do criptossistema (inversibilidade, difusão e confusão [vide item 1.2]). Como as características utilizadas por

Biham e Shamir foram determinadas a partir do DES, que é um algoritmo determinístico, estas terão suas probabilidades diferenciais reduzidas quando utilizadas contra o algoritmo a ser proposto.

3.3.2 O algoritmo SWDES

O algoritmo SWDES consiste no algoritmo básico do DES com 16 iterações com a seguinte alteração: substitui-se as trocas determinísticas Sw por trocas probabilísticas RSw, onde a condição para que uma troca RSw ocorra é a de que o número total de bites iguais à 1, em L e R, após a transformação Tr, seja par. O algoritmo SWDES pode ser representado da seguinte forma:

$SWDES = Tr_{K16} \bullet RSw \bullet Tr_{K15} \bullet ... \bullet RSw \bullet Tr_{K2} \bullet RSw \bullet Tr_{K1}$

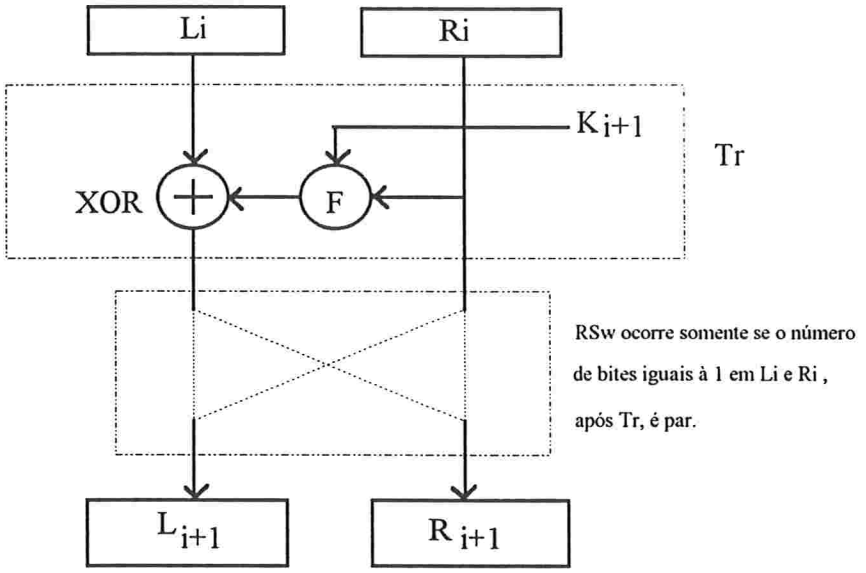


Figura 3.3a: Ilustra troca RSw probabilística

Proposição 3.3.1 O SWDES é inversível.

Demonstração:

RSW é uma involução: RSw(RSw(x)) = x.

A inversa do SWDES é calculada aplicando-se as transformações Tr seguidas das trocas RSw na ordem inversa, isto é,

$SWDES^{-1} = Tr_{K1} \bullet RSw \bullet Tr_{K2} \bullet ... \bullet RSw \bullet Tr_{K15} \bullet RSw \bullet Tr_{K16}$

Portanto, o SWDES pode ser utilizado para ciframento e deciframento com a mesma chave, de maneira idêntica ao DES.

◊

3.4 Propriedades do SWDES

Proposição 3.4.1 Seja x = (L,R) e a subchave k escolhida ao acaso com distribuição uniforme, então $P(\text{RSw(L,R)} = \text{(R,L)}) = \frac{1}{2} + \frac{1}{2^{m+1}}$ e $P(\text{RSw(L,R)} \neq \text{(R,L)}) = \frac{1}{2} - \frac{1}{2^{m+1}}$, onde L e R são respectivamente as metades esquerda e direita do criptograma na saída de cada iteração; e m = |L| =|R|.

Demonstração:

Note que RSw(L,R) = (R,L) se e só se { (o número total de bites em L e R é par) ***ou*** (o número total de bites em L e R é impar ***e*** L = R) }

Portanto $P(\text{RSw(L,R)} = \text{(R,L)}) = \frac{1}{2} + \frac{1}{2}(\frac{1}{2^m}) = \frac{1}{2} + \frac{1}{2^{m+1}}$.

Logo $P(\text{RSw(L,R)} \neq \text{(R,L)}) = 1 - P(\text{RSw(L,R)} = \text{(R,L)}) = \frac{1}{2} - \frac{1}{2^{m+1}}$.

No DES, m = 32, portanto o termo $\frac{1}{2^{m+1}}$ é muito pequeno ($\approx 1{,}16.10^{-10}$).

◊

Proposição 3.4.2 O SWDES é um criptossistema markoviano para uma definição de diferença $P' = P \oplus P^*$, supondo subchaves independentes e uniformemente aleatórias.

Demonstração:

Prova-se de maneira análoga à Proposição 2.4.5 que $\oplus$ é uma operação de grupo.

O Lema 1 de [BS91] para o DES é o seguinte: "Se a função F leva um par de entradas (em F) com diferença α em um par de saídas (de F) com diferença β, com probabilidade *p*, então qualquer par de entradas em F com diferença $X \oplus X^* = \alpha$ provoca um par de saídas em F com diferença β, pela mesma fração *p* de subchaves possíveis"

Em outras palavras o que o Lema diz é que a probabilidade de um diferencial (α,β) é igual a fração de subchaves possíveis que levam um par de mensagens com diferença α a um par de criptogramas com diferença β. A demonstração deste Lema encontra-se em [BS91] porém em linhas gerais ela consiste no seguinte: se existem *n* pares de entrada nas S-Boxes que levam $\alpha \rightarrow \beta$, então podemos determinar *n* subchaves ($S_K = S_E \oplus S_I$), cada uma levando um par (S_E, S_E^*) a um par (S_I, S_I^*), que levam ao XOR de saída β (vide Figura 2.4.1b).

O algoritmo SWDES não alterou a função F, logo o Lema 1 continua válido. Portanto $P(T' = \beta \mid P' = \alpha,\ P = \gamma)$ é independente de γ quando as subchaves são independentes e uniformemente aleatórias.

Pelo fato de que $\oplus$ é uma operação de grupo e como $P(T' = \beta \mid P' = \alpha,\ P = \gamma)$ é independente de γ quando as subchaves são independentes e uniformemente aleatórias, conclui-se que o SWDES é um criptossistema markoviano (vide item 2.4.5).
◊

Iniciamos agora a comparação do SWDES com o DES. Como não se tem conhecimento de características calculadas para o SWDES, iremos utilizar para o SWDES as mesmas características usadas no DES. Portanto iremos considerar o caso em que o SWDES se comporta de maneira análoga ao DES quanto ao número de trocas realizadas. Mostraremos o que ocorre ao se tentar atacar o SWDES por criptoanálise diferencial usando as características disponíveis para o DES.

Lema 3.4.1 Consideremos o caso em que o SWDES se comporta de maneira análoga ao DES, em relação ao número de trocas realizadas. Seja p_i a probabilidade de que uma entrada em F com diferença α_i cause uma saída em F com diferença β_i, em cada iteração i do SWDES. Então a probabilidade diferencial da iteração i do SWDES é igual a
$P(\mathrm{RSw}(L_i, R_i) = (R_i, L_i)$ e $(\mathrm{RSw}(L_i^*, R_i^*) = (R_i^*, L_i^*)$ e $\alpha_i \to \beta_i) \cong p_i(\frac{1}{4} + \frac{1}{2^{m+1}})$, onde $m = |L| = |R|$.

Demonstração:

A troca RSw não possui nenhuma relação com a função F. Portanto a probabilidade de que α_i cause uma saída β_i em F é independente da troca RSw.

Após a função F, desejamos que a característica se comporte de maneira análoga à uma característica do DES. Portanto em cada mensagem do par de ciframentos deve ocorrer a troca RSw. A probabilidade de que a troca ocorra em cada ciframento do par é, de acordo com a Proposição 3.4.1, igual a $(\frac{1}{2} + \frac{1}{2^{m+1}})^2 \cong (\frac{1}{4} + \frac{1}{2^{m+1}})$.

A troca RSw deve ocorrer após a função F, portanto a probabilidade diferencial da iteração i do SWDES é aproximadamente igual a $p_i\ (\frac{1}{4} + \frac{1}{2^{m+1}})$.
◊

Teorema 3.4.1 Consideremos uma característica do DES com n iterações com probabilidade diferencial igual a p. Esta característica quando usada contra o SWDES com n iterações possui probabilidade diferencial igual a $(\frac{1}{4}+\frac{1}{2^{m+1}})^{n-1}p$, onde m = |L| =|R|.

Demonstração:

Pelo Lema 3.4.1, a probabilidade diferencial de cada iteração do SWDES, quando este se comporta de maneira análoga ao DES, é $p_i\ (\frac{1}{4}+\frac{1}{2^{m+1}})$, onde p_i é a probabilidade diferencial de cada iteração no DES. Como o DES é um criptossistema markoviano (vide Proposição 2.4.5) então $p=\prod_{i=1}^{n} p_i$. O SWDES também é um criptossistema markoviano (vide Proposição 3.4.2), portanto a probabilidade diferencial da característica de n iterações quando aplicada ao SWDES é igual a

$$p_1\prod_{i=2}^{n} p_i(\frac{1}{4}+\frac{1}{2^{m+1}}) = (\frac{1}{4}+\frac{1}{2^{m+1}})^{n-1}\prod_{i=1}^{n} p_i = (\frac{1}{4}+\frac{1}{2^{m+1}})^{n-1}p.$$

Para o SWDES, m = 32 (vide Proposição 3.4.1) e então pode-se considerar que a probabilidade diferencial da característica quando aplicada ao SWDES é aproximadamente igual a $\frac{p}{4^{n-1}}$.

◊

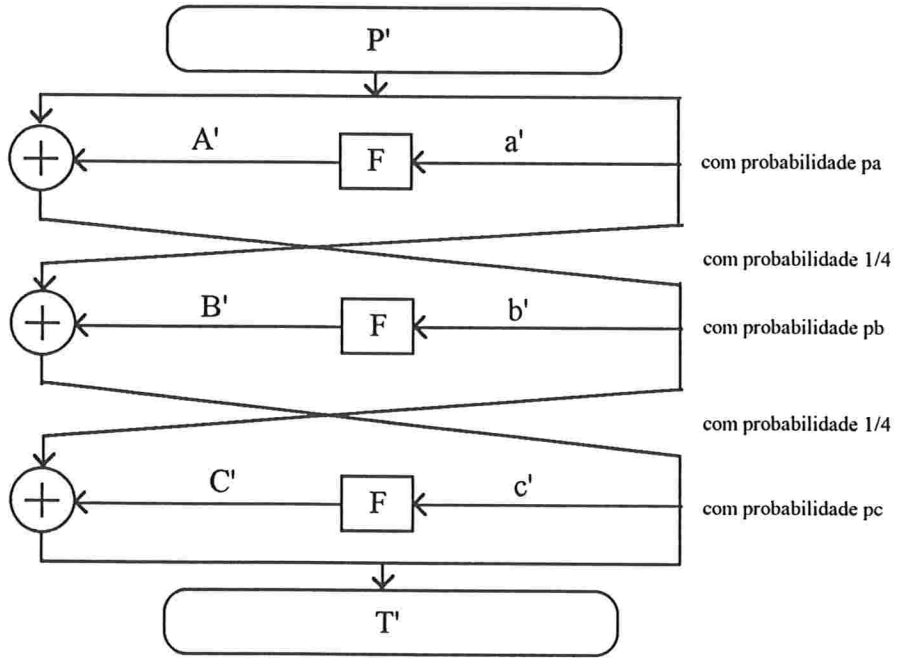


Figura 3.4a: Exemplo de uma característica do SWDES com três iterações e de comportamento análogo ao DES.

Proposição 3.4.3 Seja p a probabilidade diferencial de uma característica para o DES com n iterações. Então o SWDES com n iterações e o DES com $n(1+\log_p 4^{-n+1})$ possuem a mesma probabilidade diferencial.

Demonstração:

Suponha que a probabilidade diferencial para o DES com kn iterações é p^k, onde k é um inteiro positivo. A probabilidade diferencial de uma característica de n iterações, quando aplicada ao SWDES, é igual a $\frac{p}{4^{n-1}}$ (vide Teorema 3.4.1).

Desejamos calcular k, de modo que o DES e o SWDES possuam as mesmas probabilidades diferenciais. Para tal devemos resolver a seguinte equação: $p^k = \frac{p}{4^{n-1}}$.

Logo $k = (1+\log_p 4^{-n+1})$. Portanto o SWDES com n iterações e o DES com $n(1+\log_p 4^{-n+1})$ possuem a mesma probabilidade diferencial.

◊

Suponhamos que $p = 1{,}0.10^{-10}$. O SWDES com 16 iterações possui a mesma probabilidade diferencial que o DES com 31 iterações.

Veja outros exemplos no capítulo 4.

3.5 Resultados Experimentais

Alguns experimentos foram realizados com o SWDES para verificar a uniformidade do número de trocas realizadas entre as metades esquerda e direita após cada transformação Tr. O procedimento consistiu em analisar amostras divididas em três grupos, cada grupo com cinco conjuntos de amostras. Em cada grupo foram observados o número de trocas realizadas em cada iteração e o número de trocas realizadas por operação de ciframento.

No primeiro grupo (A), fixa-se a mensagem e esta é cifrada com várias chaves de ciframento escolhidas ao acaso. No segundo grupo (B), fixa-se a chave de ciframento e esta é utilizada para o ciframento de várias mensagens escolhidas ao acaso. No terceiro grupo (C), várias mensagens e a suas respectivas chaves de ciframento são escolhidas ao acaso.

Cada grupo contém cinco conjuntos de amostras, de cardinalidades respectivamente iguais a 5000, 5500, 6000, 6500 e 7000. Em cada conjunto de amostras foi executado o procedimento correspondente ao seu grupo. Os resultados obtidos estão representados nos gráficos a seguir e tabelados no apêndice B.

Grupo A: Mensagem Fixa e Chaves Aleatórias

Tamanho da Amostra (número de ciframentos realizados)	Mensagem Fixa (notação hexadecimal) (inicialmente escolhida ao acaso e mantida fixa durante os ciframentos)
5000	5b b4 3a 42 9c f0 e6 0e
5500	82 3e 58 d9 67 38 dd 9e
6000	e3 08 69 02 be e4 96 3b
6500	23 e9 08 63 5a af 22 93
7000	9e 0a 99 56 81 dd 6f f7

Distribuição do Número de Trocas Realizadas por Iteração

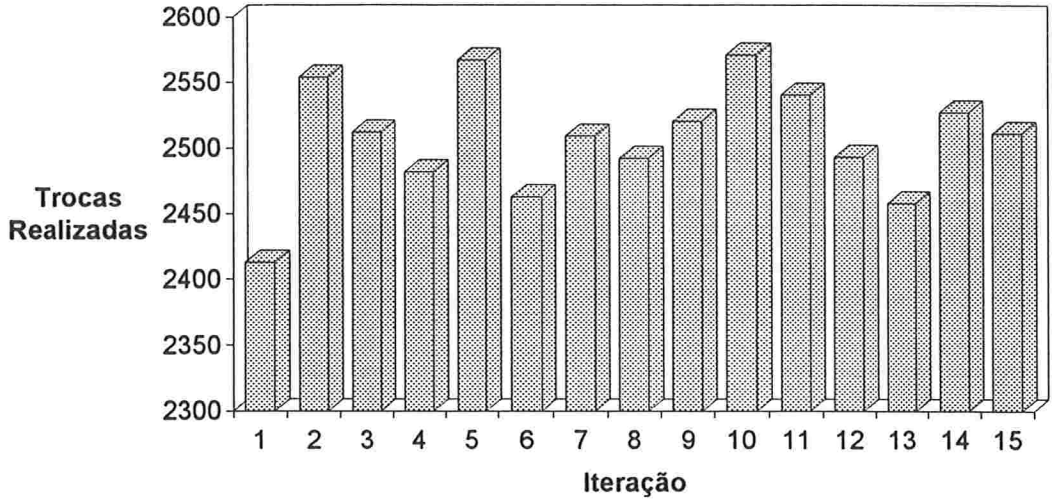


Figura 3.5.1: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5000 Ciframentos (número médio de trocas esperado: 2500).
número médio de trocas: 2507,47

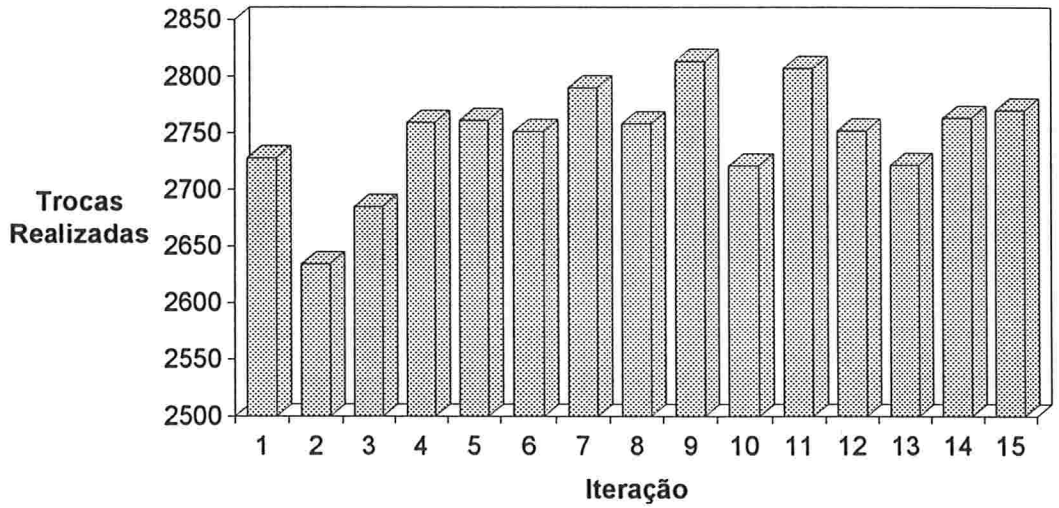


Figura 3.5.2: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5500 Ciframentos (número médio de trocas esperado: 2750).
número médio de trocas: 2747,6

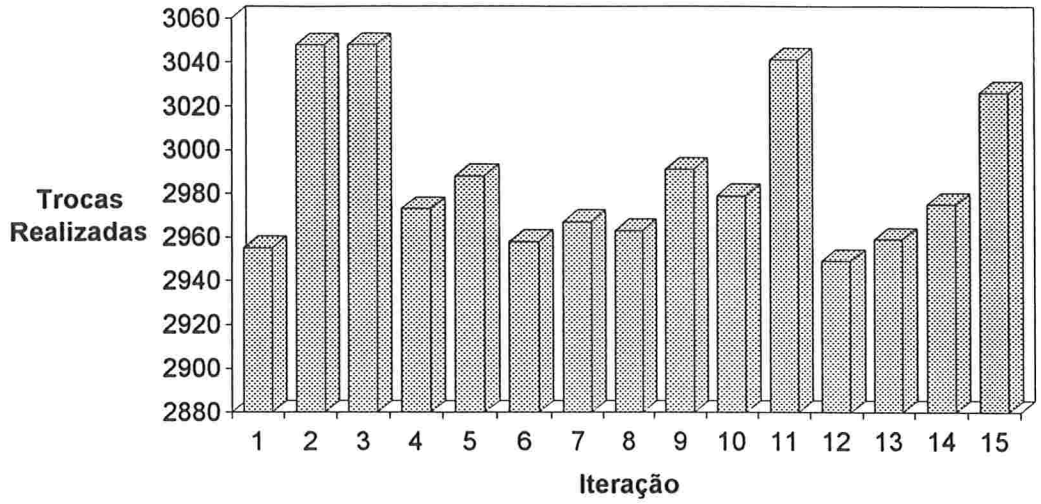


Figura 3.5.3: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6000 Ciframentos (número médio de trocas esperado: 3000).
número médio de trocas: 2988

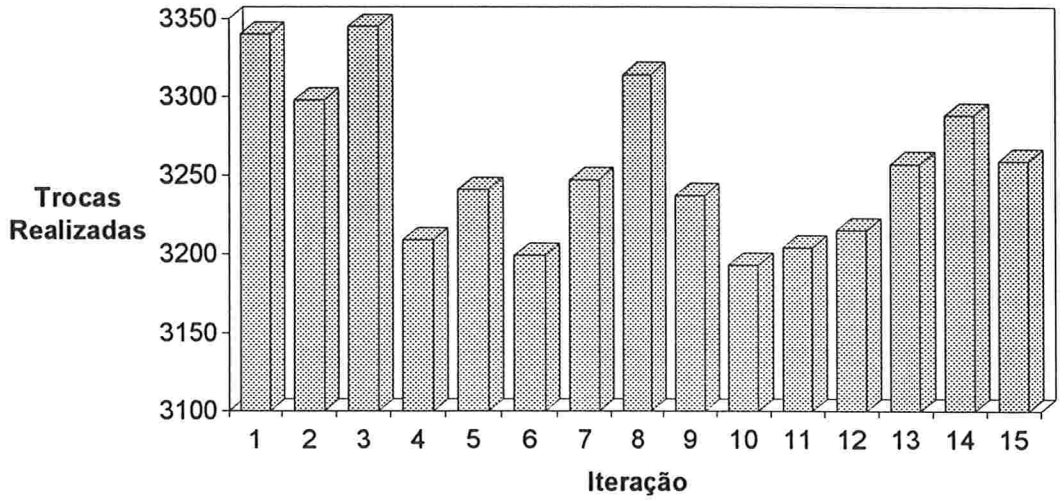


Figura 3.5.4: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6500 Ciframentos (número médio de trocas esperado: 3250).
número médio de trocas: 3256,4

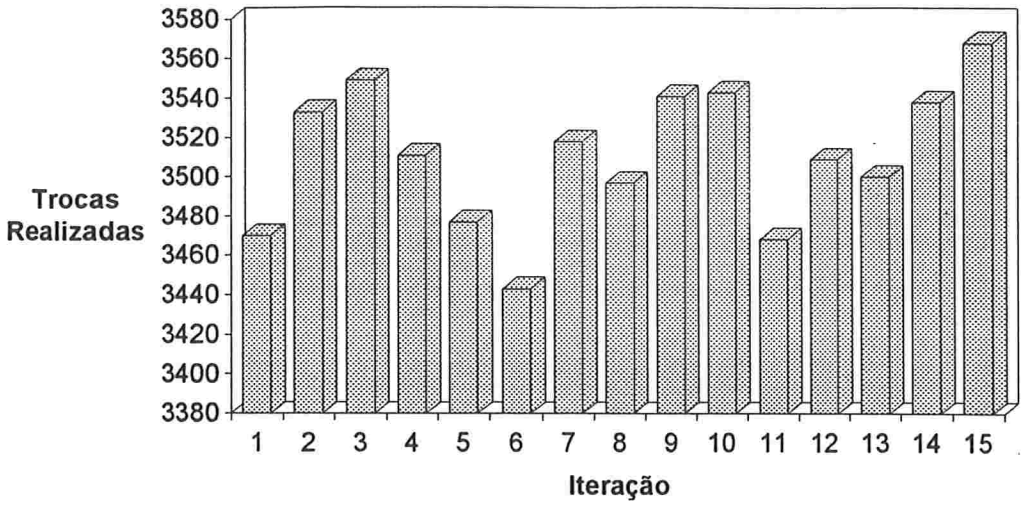


Figura 3.5.5: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 7000 Ciframentos (número médio de trocas esperado: 3500)
número médio de trocas: 3511

Distribuição do Número de Trocas Realizadas por Ciframento

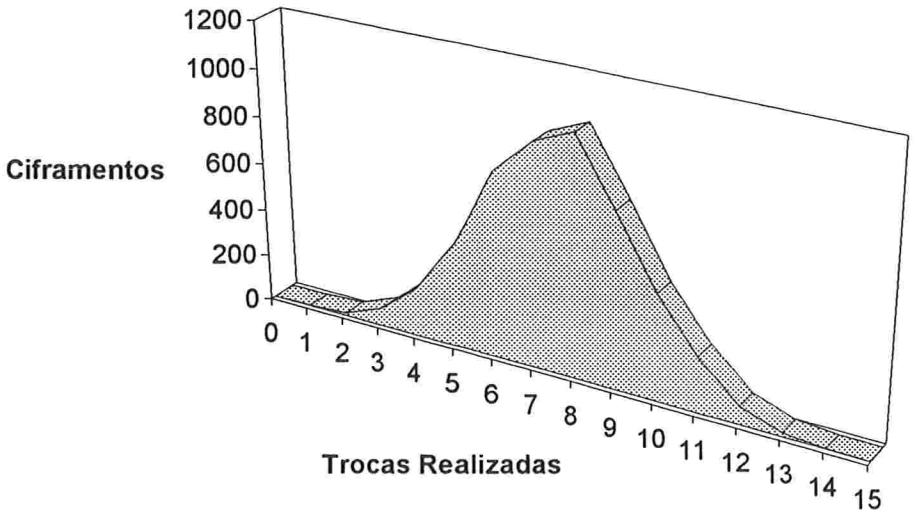


Figura 3.5.6: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

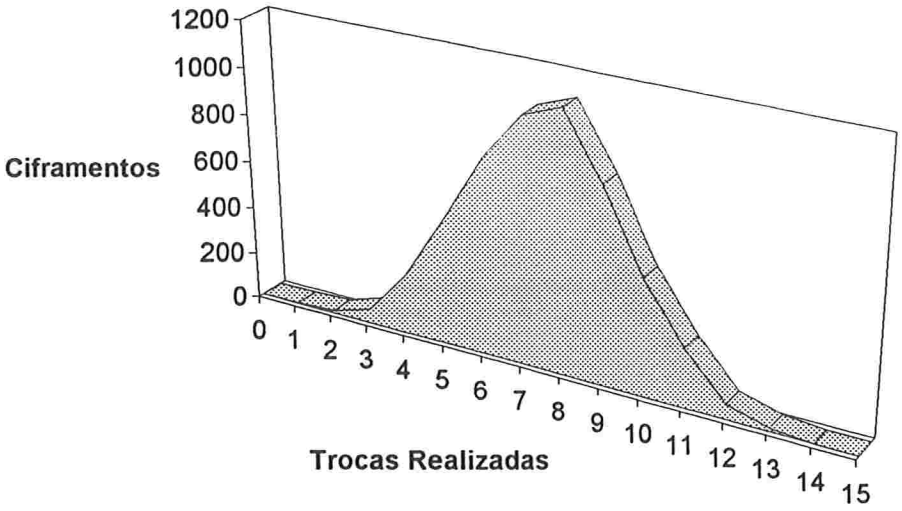


Figura 3.5.7: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

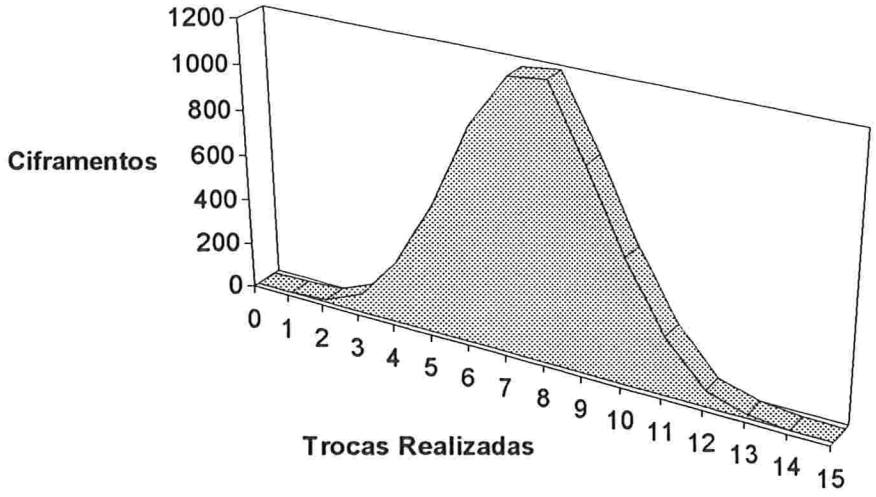


Figura 3.5.8: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

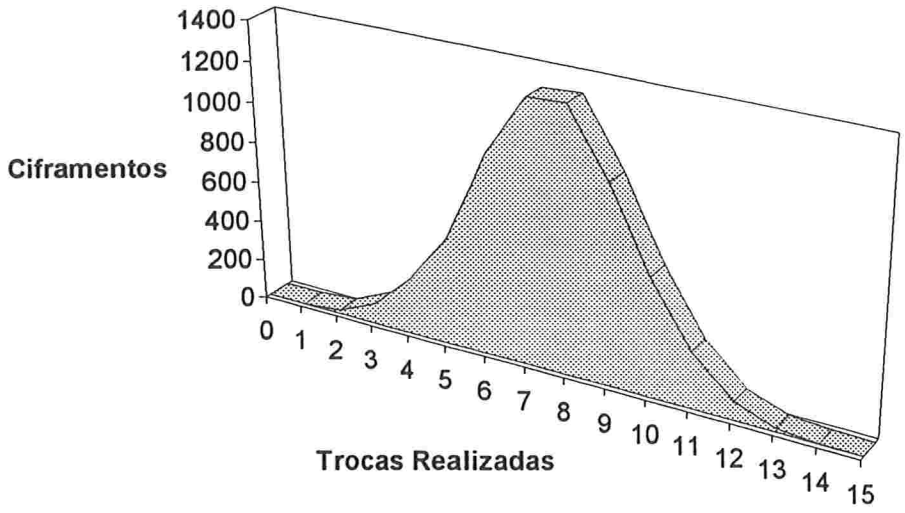


Figura 3.5.9: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

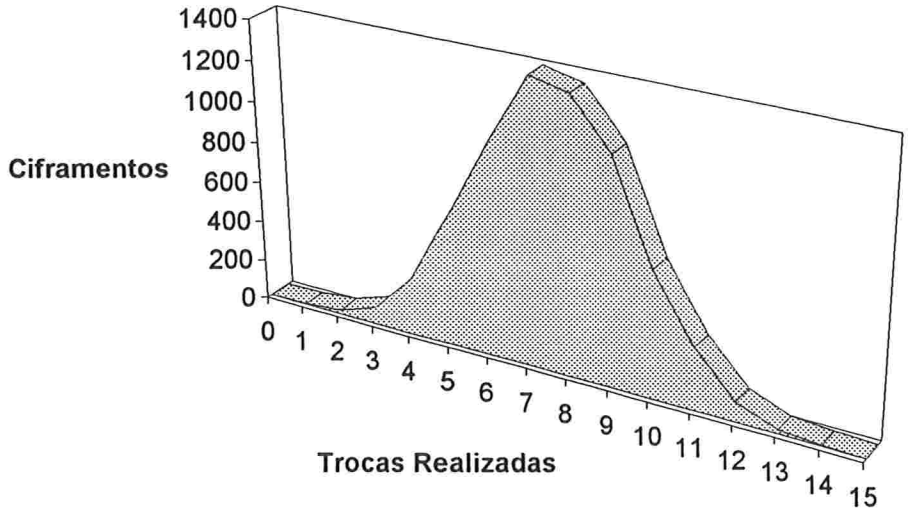


Figura 3.5.10: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 7000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

Grupo B: Chave Fixa e Mensagens Aleatórias

Tamanho da Amostra (número de ciframentos realizados)	Chave Fixa (notação hexadecimal) (inicialmente escolhida ao acaso e mantida fixa durante os ciframentos)
5000	4a 21 ff 77 ca ef 15 c5
5500	cb d4 81 6a db 7c fa a9
6000	2b 9e 92 93 32 28 b3 46
6500	6c 7f 30 f4 cd f3 3f 9d
7000	e6 a0 c2 e7 f4 21 8c 02

Distribuição do Número de Trocas Realizadas por Iteração

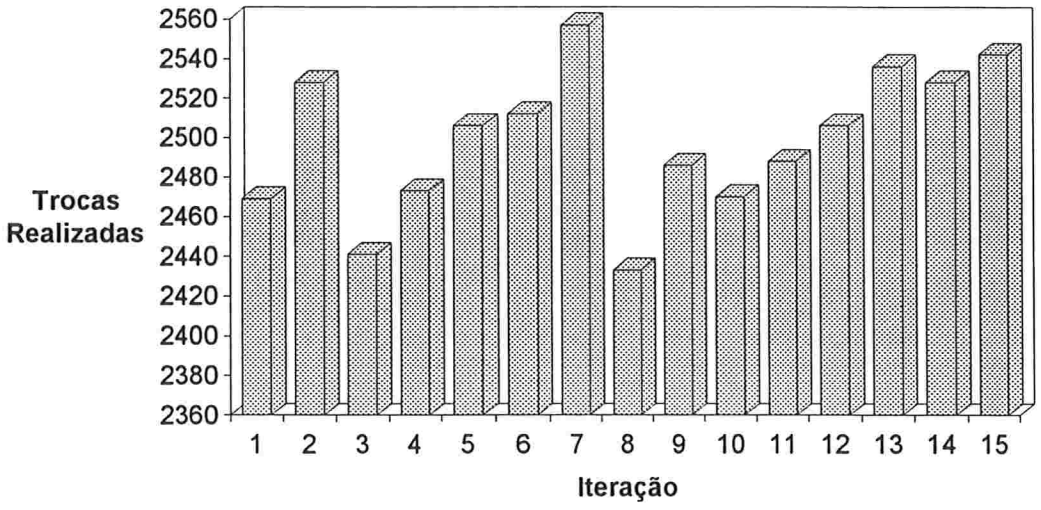


Figura 3.5.11: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5000 Ciframentos (número médio de trocas esperado: 2500)
número médio de trocas: 2498,33

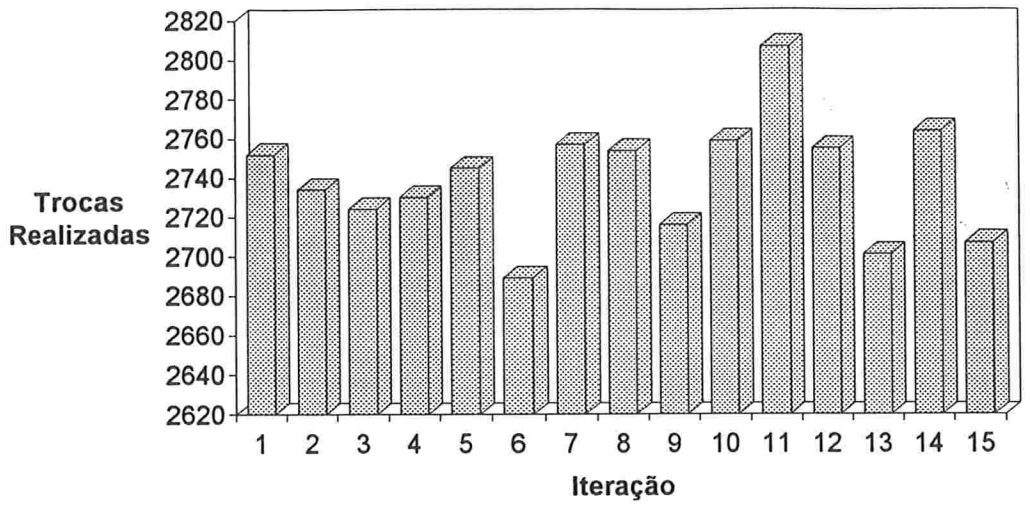


Figura 3.5.12: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5500 Ciframentos (número médio de trocas esperado: 2750)
número médio de trocas: 2739,6

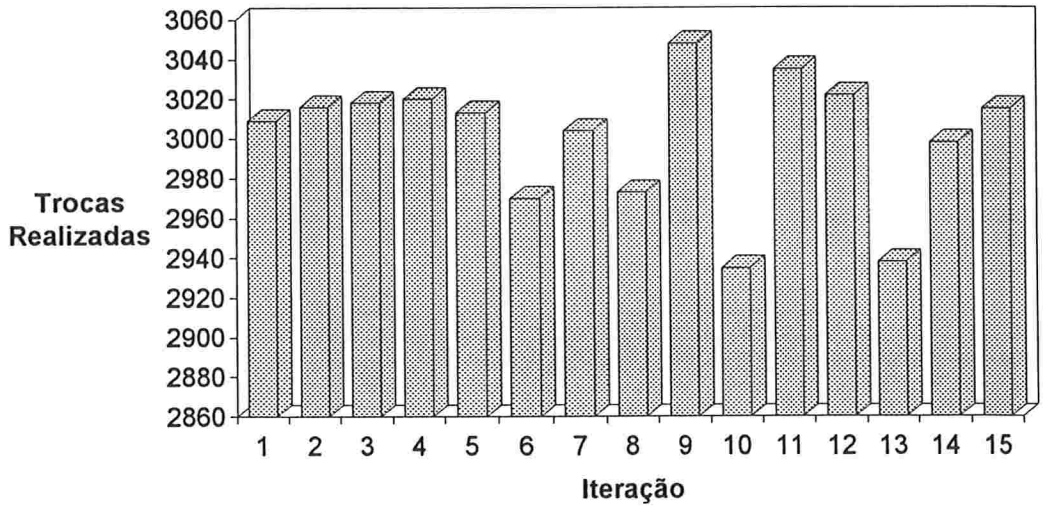


Figura 3.5.13: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6000 Ciframentos (número médio de trocas esperado: 3000)
número médio de trocas: 3000,93

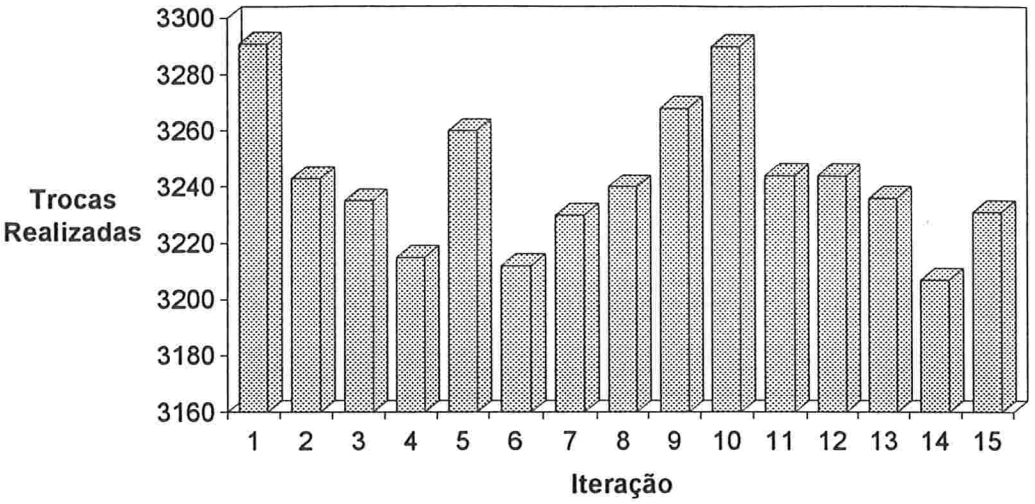


Figura 3.5.14: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6500 Ciframentos (número médio de trocas esperado: 3250)
número médio de trocas: 3243,07

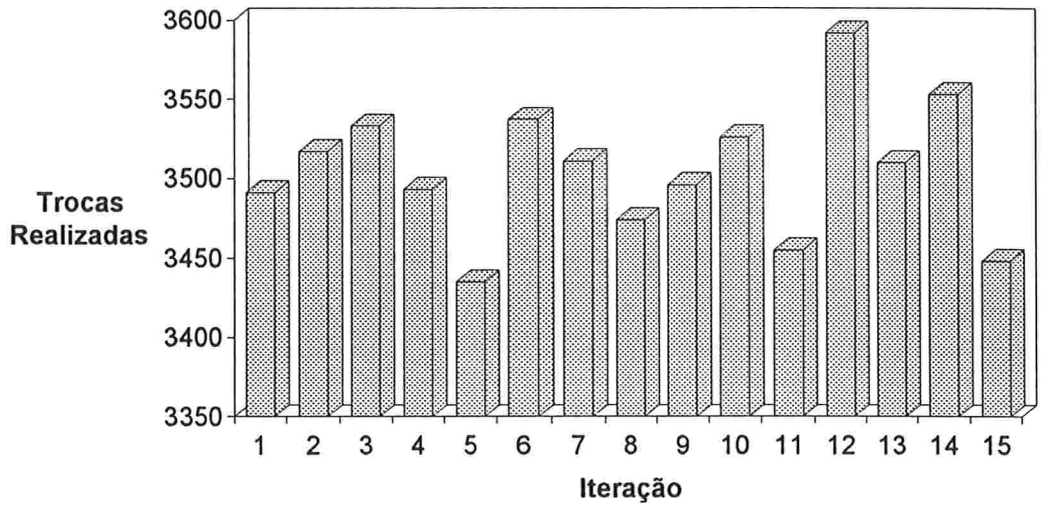


Figura 3.5.15: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 7000 Ciframentos (número médio de trocas esperado: 3500)
número médio de trocas: 3504,73

Distribuição do Número de Trocas Realizadas por Ciframento

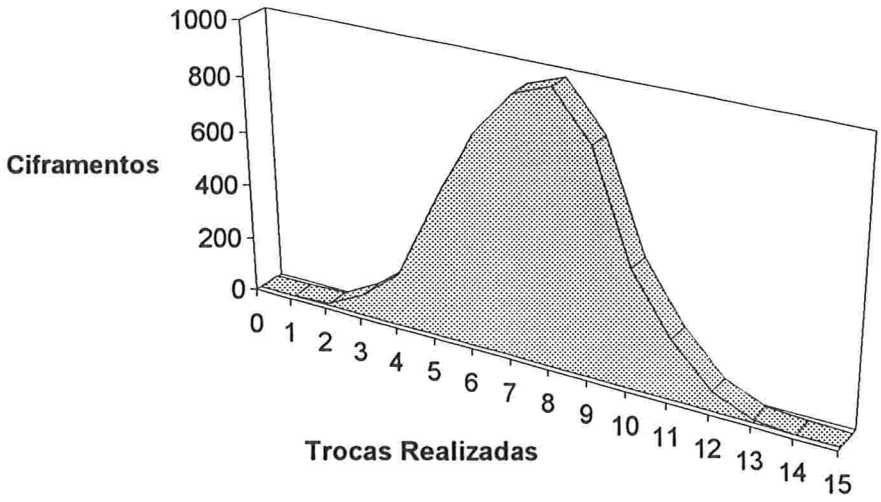


Figura 3.5.16: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

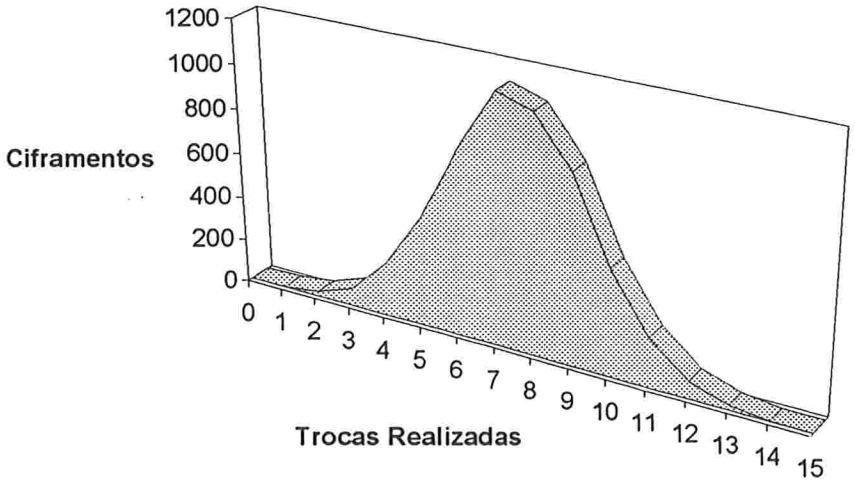


Figura 3.5.17: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

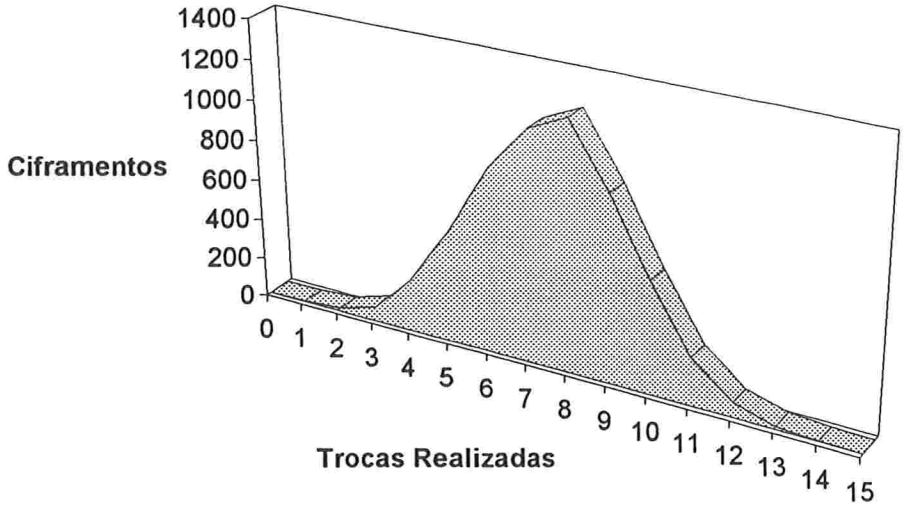


Figura 3.5.18: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

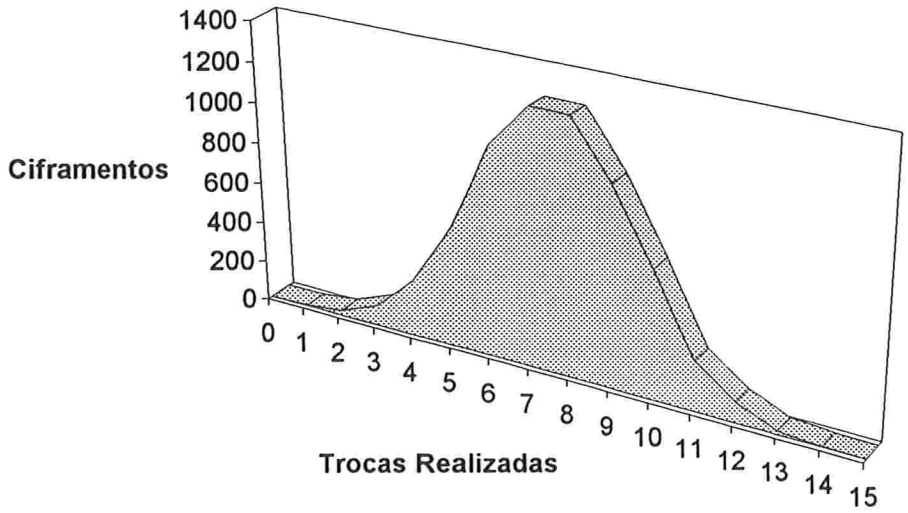


Figura 3.5.19: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

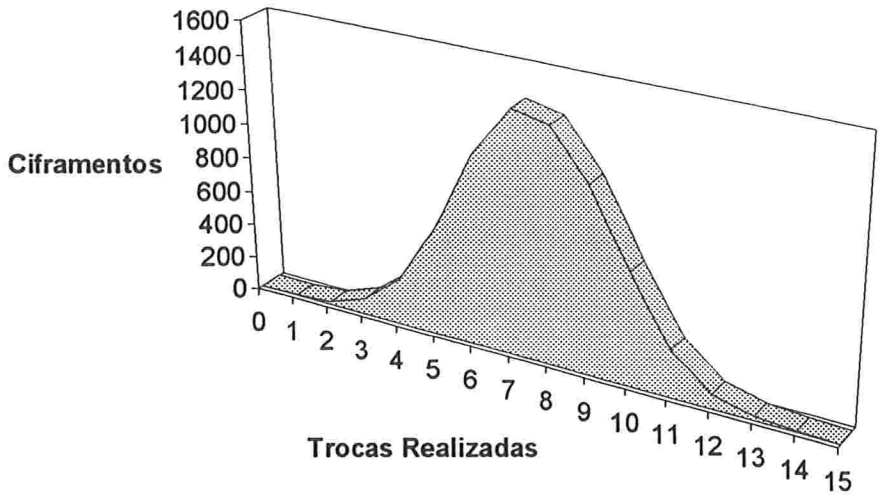


Figura 3.5.20: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 7000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

Grupo C: Mensagens e Chaves Aleatórias

Distribuição do Número de Trocas Realizadas por Iteração

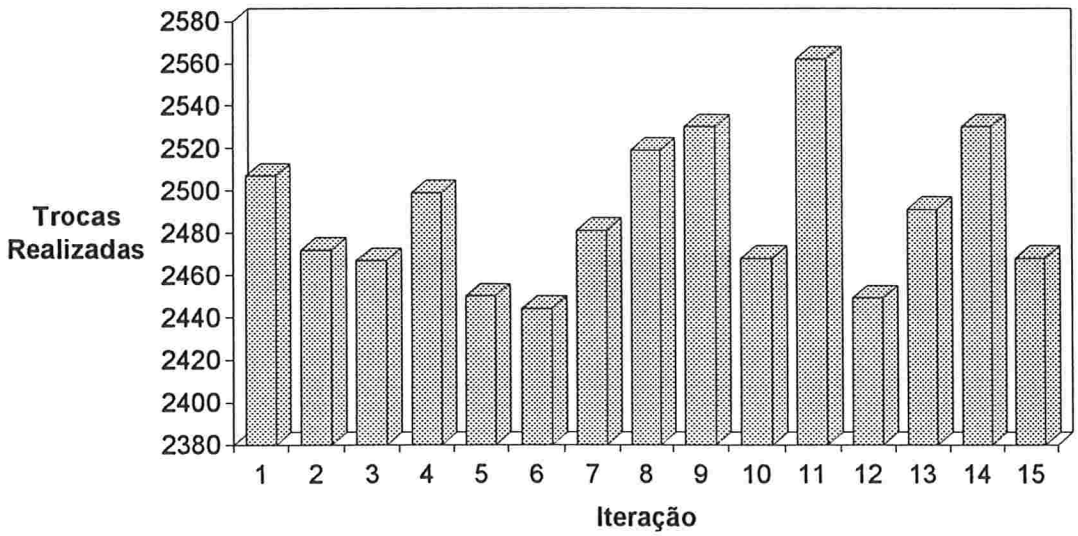


Figura 3.5.21: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5000 Ciframentos (número médio de trocas esperado: 2500)
número médio de trocas: 2489,13

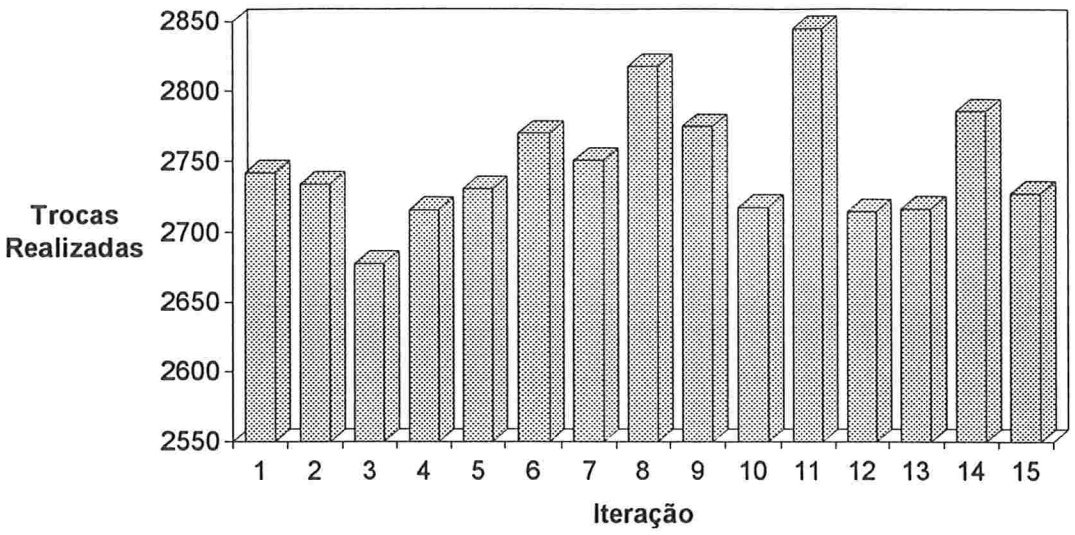


Figura 3.5.22: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 5500 Ciframentos (número médio de trocas esperado: 2750)
número médio de trocas: 2748,27

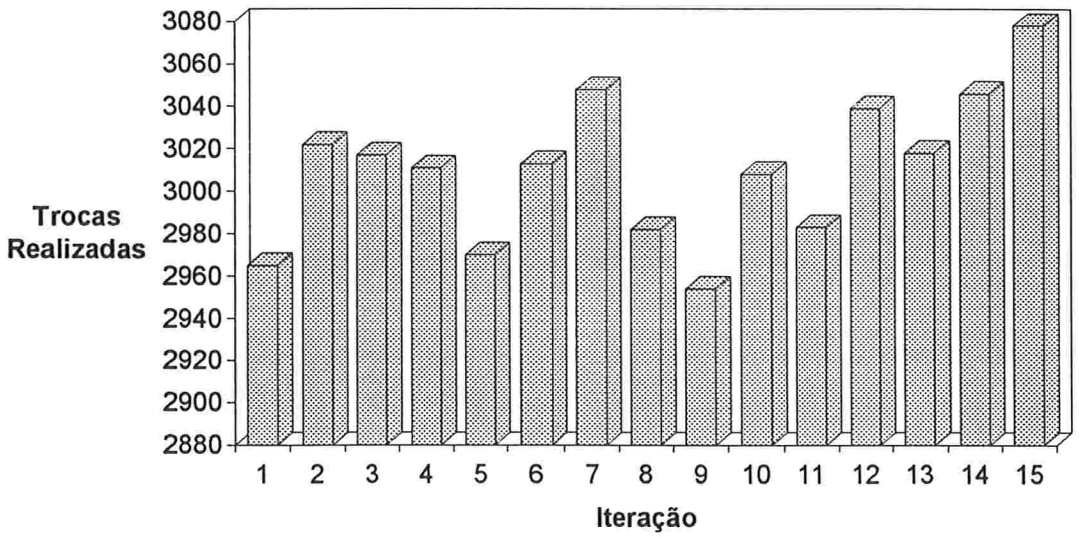


Figura 3.5.23: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6000 Ciframentos (número médio de trocas esperado: 3000)
número médio de trocas: 3010,27

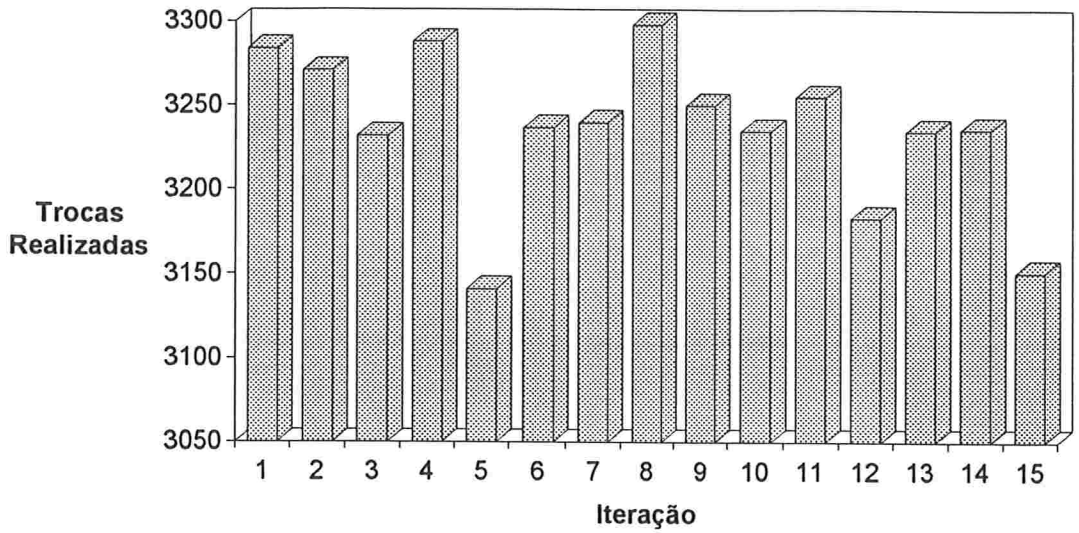


Figura 3.5.24: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 6500 Ciframentos (número médio de trocas esperado: 3250)
número médio de trocas: 3235,73

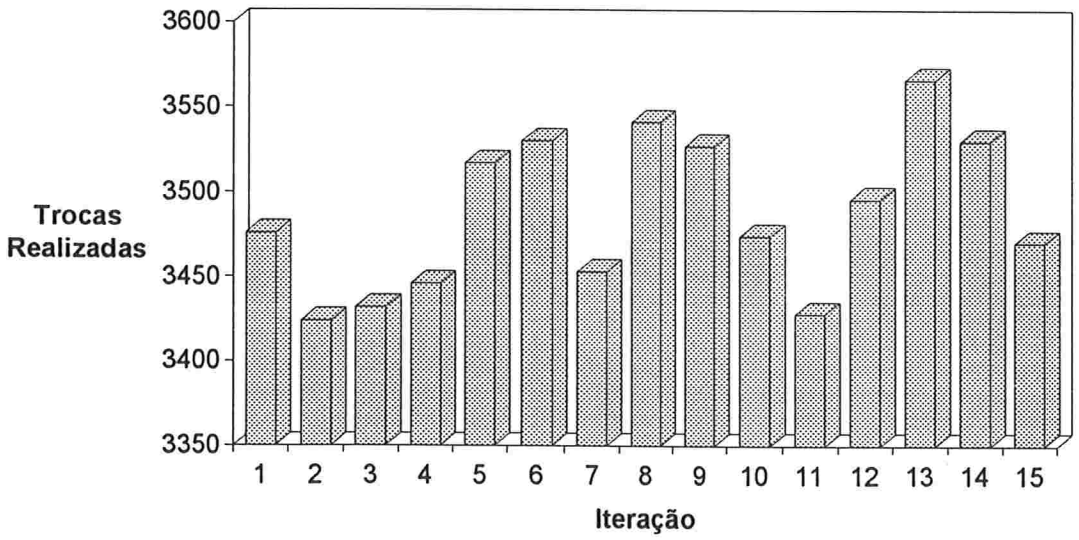


Figura 3.5.25: Distribuição do Número de Trocas Realizadas por Iteração na Amostra de 7000 Ciframentos (número médio de trocas esperado: 3500)
número médio de trocas: 3487,33

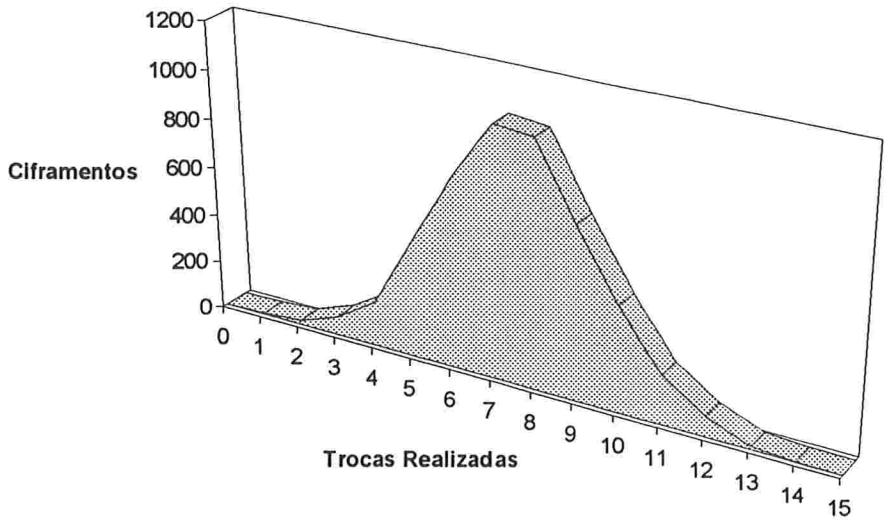


Figura 3.5.26: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

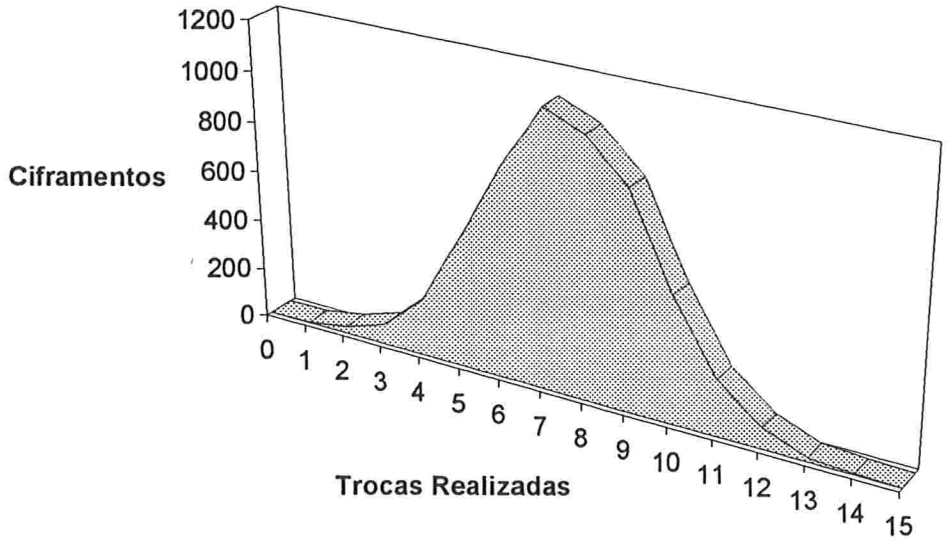


Figura 3.5.27: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 5500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

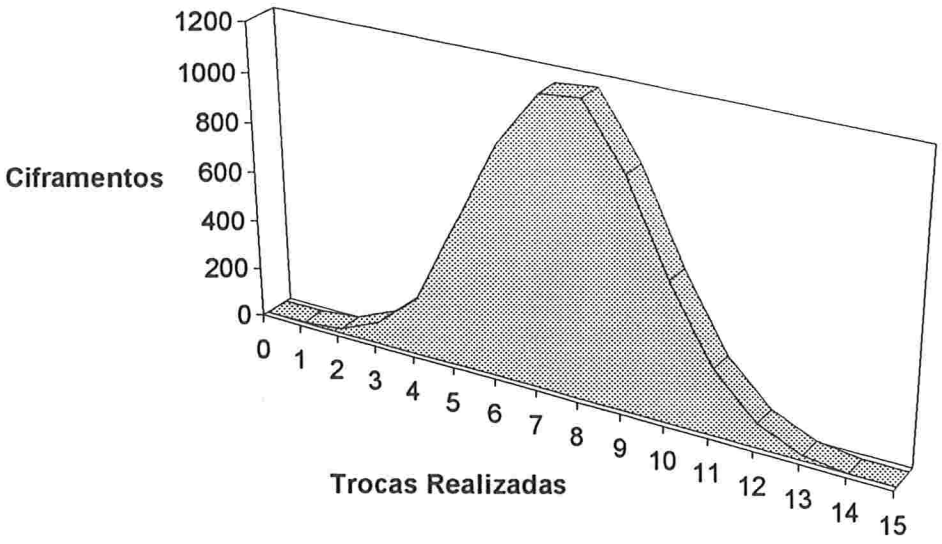


Figura 3.5.28: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

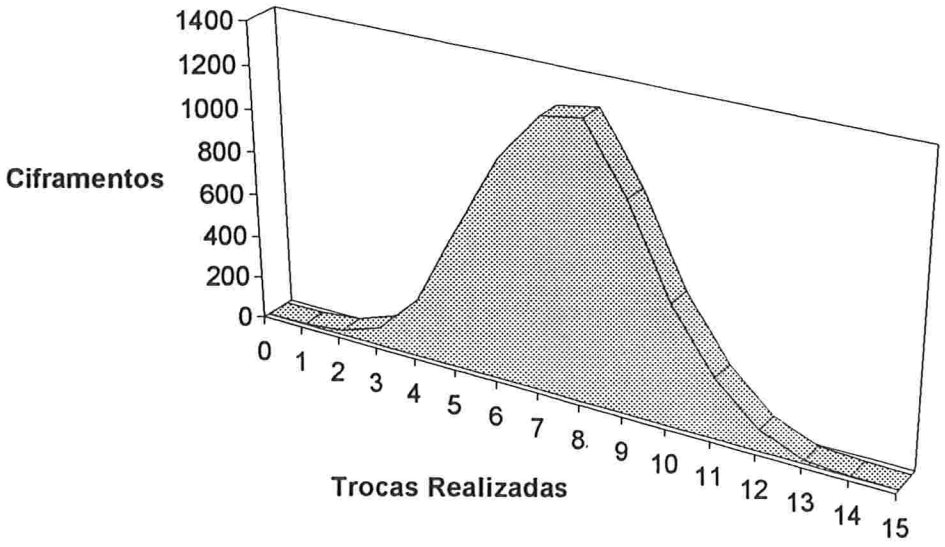


Figura 3.5.29: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 6500 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

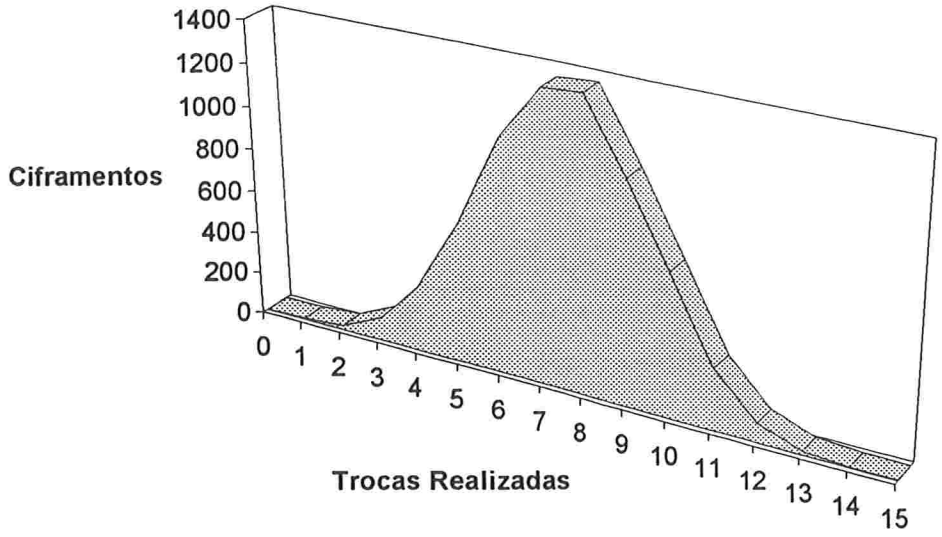


Figura 3.5.30: Distribuição do Número de Trocas Realizadas por Ciframento na Amostra de 7000 Ciframentos (número médio de trocas esperado: 7)
número médio de trocas: 7

Observando-se os resultados acima verificamos que em média são realizados 7 trocas ao longo de cada ciframento e que o número de trocas está bem distribuído ao longo das iterações. Isto de certa forma era esperado devido às características de projeto das Caixas de Substituição (S-Boxes), que possuem comportamento pseudo-aleatório (vide demonstração do Teorema 2.4.5.1). Portanto ao se introduzir a troca com probabilidade de aproximadamente 0.5, reduzimos o número provável de trocas por ciframento em 50% (no DES ocorrem 15 trocas). Os dados acima permitem verificar que o algoritmo não possui mudança de comportamento na faixa de dados escolhida e pode-se esperar, devido à pseudo-aleatoriedade da função F (vide demonstração do Teorema 2.4.5.1), que isto também ocorra para outras faixas.

Proposição 3.5.1 O SWDES conserva o efeito avalanche.
Demonstração:

Para o DES, Konheim [K81,pág.262] demonstra que o efeito avalanche é atingido após 3-4 iterações. A partir dos resultados acima, concluimos que o SWDES conserva o efeito avalanche pois em média ocorrem 7 trocas por ciframento. Deve-se notar que o SWDES possui 16 iterações.

◊

Capítulo 4

Conclusões

A maneira mais fácil de aumentar a resistência do DES contra a criptoanálise diferencial é aumentar o número de iterações que o algoritmo possui [KT93] pois desta forma, é necessária uma característica com um número elevado de iterações, com conseqüente redução da probabilidade diferencial. Porém este método apresenta a desvantagem de aumentar o tempo das operações de ciframento e deciframento.

Biham e Shamir em seu ataque ao DES com 16 iterações [BS92] usam como base principal uma característica de 13 iterações com probabilidade diferencial igual a aproximadamente $2^{-47.2}$. De acordo com [Kn92], Biham e Shamir utilizam as melhores características disponíveis, até o momento, para um ataque ao DES.

De acordo com as propriedades do sistema obtido após a introdução da alteração proposta (o algoritmo SWDES), ao se aplicar, num ataque por criptoanálise diferencial, a característica utilizada por Biham e Shamir, esta terá sua probabilidade diferencial reduzida a $(\frac{1}{4})^{13-1}.(2^{-47.2}) = 2^{-71.2}$. Consequentemente o sucesso do ataque é reduzido consideravelmente.

Considerando que a probabilidade diferencial para o DES com n iterações* é $(\frac{1}{234})^{n/2}$ (valores correspondentes na linha 1 da tabela 4.1), utilizando a característica iterativa utilizada por Biham e Shamir em seu ataque ao DES com 16 iterações (vide Figura 3.1a), a tabela a seguir ilustra a equivalência entre o número de iterações necessárias para que uma característica utilizada contra o DES e o SWDES tenha a mesma probabilidade diferencial (vide Proposição 3.4.3).

---

* para n = 6 itera-se a característica da Figura 3.1a 3 vezes, para n = 8 itera-se 4 vezes e assim sucessivamente até n = 13 onde itera-se a característica 6,5 vezes.

probabilidade diferencial	$2^{-23.6}$	$2^{-31.48}$	$2^{-39.35}$	$2^{-47.2}$
SWDES	5	6	8	10
DES	6	8	10	13

Tabela 4.1: Número Mínimo de Iterações no DES e SWDES Com a Mesma Probabilidade Diferencial

Portanto o SWDES é mais forte contra a criptoanálise diferencial que o DES (o SWDES precisa de um número menor de iterações para atingir a mesma probabilidade diferencial) e o tempo de ciframento não é alterado significativamente pois a verificação dos bites em cada iteração não é uma operação que consome muito tempo e pode ser realizada em tempo linear. A robustez do SWDES com 13 iterações é equivalente à robustez do DES com 20 iterações, considerando-se a característica citada no parágrafo anterior.

O SWDES deve ser implementado sempre com mais de 6 iterações para garantir que o efeito avalanche seja mantido, pois neste caso em média mais de 3 trocas por ciframentos irão ocorrer.

Implementações do DES em software podem ser facilmente modificadas para o SWDES.

Nas implementações do DES em hardware, o circuito responsável pela transformação Tr pode ser mantido. O circuito responsável pela troca Sw também pode ser mantido, porém após este circuito deve-se acoplar um outro circuito (Sw2) que verifica se o número de bites iguais a 1 é par ou ímpar e desfaz a troca realizada caso necessário (vide Figura 4.1).

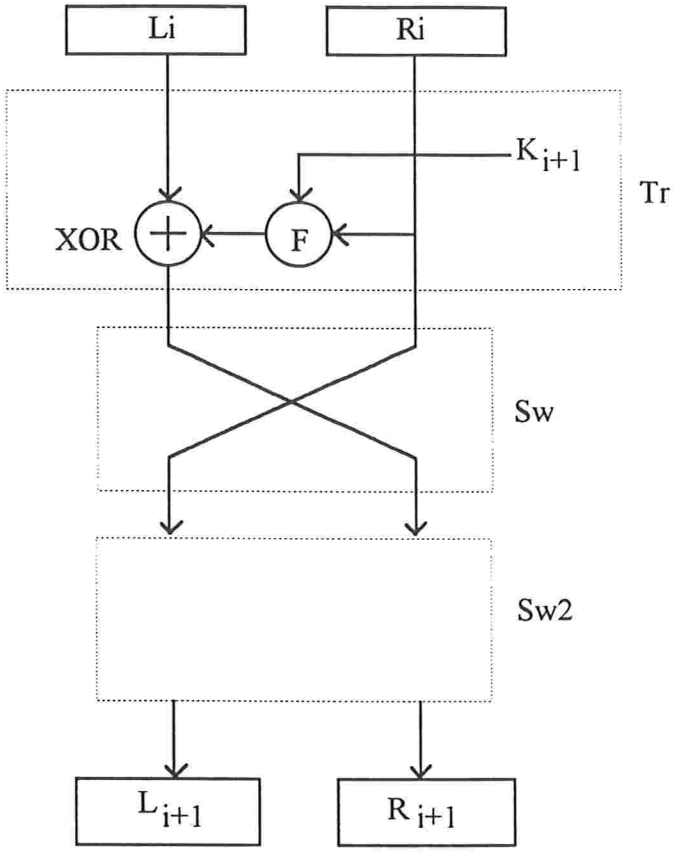


Figura 4.1: Ilustra possível implementação do SWDES em hardware

O circuito para a verificação do número de bites iguais a 1 consiste em um circuito verificador de paridade, que é um dos mais fáceis circuitos de serem implementados. Desta forma a implementação do SWDES não possui um custo elevado.

Apresentamos a seguir sugestões para futuros trabalhos na mesma linha de estudo da proposta aqui apresentada:

- Composição do SWDES com alterações nas Caixas de Substituição.
- Composição do SWDES com o RDES [KT93].
- Manter a troca Sw determinística mas introduzir uma troca probabilística entre as duas metades de R, imediatamente antes da Função F.

Apêndice A

Tabelas do DES

Observações:

1) A menos que se diga o contrário, quando for necessário identificar um bit de uma sequência de bites sempre consideraremos o sentido da esquerda para a direita. Por exemplo, bit 1 de 1000 é 1, bit 2 de 1011 é 0, bit 3 de 1101111 é 0.

2) n_b indica um binário. Por exemplo $10_b = 2$, $101_b = 5$.

Tabela A1: Número de deslocamentos circulares à esquerda realizados em cada iteração do processo de geração de subchaves

No. da Iteração	No. de Deslocamentos
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Tabela A2: Permutação Inicial.

Deve-se ler a tabela da seguinte forma: bit 1 da entrada vai para o bit 58 da saída, bit 2 da entrada vai para o bit 50 da saída, ..., bit 9 da entrada vai para o bit 60 da saída, etc.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabela A3: Inversa da Permutação Inicial.

Deve-se ler a tabela da seguinte forma: bit 1 da entrada vai para o bit 40 da saída, bit 2 da entrada vai para o bit 8 da saída, ..., bit 9 da entrada vai para o bit 39 da saída, etc.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tabela A4: Permutação Escolha 1

Deve-se ler a tabela da seguinte forma: bit 1 da saída corresponde ao bit 57 da entrada, bit 2 da saída corresponde ao bit 49 da entrada, ..., bit 56 da saída corresponde ao bit 4 da entrada.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Tabela A5: Permutação Escolha 2

Deve-se ler a tabela da seguinte forma: o bit 1 da saída corresponde ao bit 14 da entrada, o bit 2 da saída corresponde ao bit 17 da entrada, ..., o bit 47 da saída corresponde ao bit 29 da entrada e o bit 48 corresponde ao bit 32 da entrada.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tabela A6: Expansão E

Deve-se ler a tabela da seguinte forma: bit 1 da saída corresponde ao bit 32 da entrada, bit 2 da saída corresponde ao bit 1 da entrada, bit 3 da saída corresponde ao bit 2 da entrada, ..., bit 7 da saída corresponde ao bit 4 da entrada, ..., os 2 últimos bites da saída correspondem respectivamente ao bites 32 e 1 da entrada.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tabela A7: Permutação P

Deve-se ler a tabela da seguinte forma: o bit 1 da saída corresponde ao bit 16 da entrada, o bit 2 da saída corresponde ao bit 7 da entrada, ..., bit 5 da saída corresponde ao bit 29 da entrada, ..., bit 32 da saída corresponde ao bit 25 da entrada.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabela A8: Caixas de Substituição (S-Boxes).

As linhas e colunas de uma Caixa de Substituição são numeradas respectivamente de 0 a 3 e de 0 a 15. Suponhamos que a seguinte entrada ocorre em S1: 110000_b. O primeiro e o último bit (da esquerda para a direita) indicam a linha da tabela que se deve olhar. Os restantes indicam a coluna. Neste caso a linha é 2 (= 10_b) e a coluna é 8 (= 1000_b). Portanto a saída é $15 = 1111_b$.

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Apêndice B

Resultados Experimentais

Tabela B1: (Grupo A) Amostra de tamanho 5000. (Figura 3.5.1)
Mensagem Fixa: 5B B4 3A 42 9C F0 E6 0Ex
número médio de trocas esperado por iteração: 2500
número médio de trocas: 2507,47

Iteração	Trocas Realizadas
1	2413
2	2554
3	2512
4	2482
5	2567
6	2463
7	2509
8	2492
9	2520
10	2571
11	2540
12	2493
13	2458
14	2527
15	2511

Tabela B2: (Grupo A) Amostra de tamanho 5000. (Figura 3.5.6)
Mensagem Fixa: 5B B4 3A 42 9C F0 E6 0Ex
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 15

Trocas Realizadas	Ciframentos
0	0
1	3
2	11
3	76
4	209
5	443
6	787
7	941
8	1011
9	741
10	447
11	231
12	76
13	19
14	3
15	2

Tabela B3: (Grupo A) Amostra de tamanho 5500. (Figura 3.5.2)
Mensagem Fixa: 82 3E 58 D9 67 38 DD 9Ex
número médio de trocas esperado por iteração: 2750
número médio de trocas: 2747,6

Iteração	Trocas Realizadas
1	2728
2	2634
3	2685
4	2759
5	2761
6	2751
7	2790
8	2758
9	2813
10	2721
11	2807
12	2752
13	2722
14	2763
15	2770

Tabela B4: (Grupo A) Amostra de tamanho 5500. (Figura 3.5.7)
Mensagem Fixa: 82 3E 58 D9 67 38 DD 9Ex
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	2
2	11
3	62
4	258
5	535
6	829
7	1034
8	1100
9	836
10	500
11	252
12	65
13	15
14	1
15	0

Tabela B5: (Grupo A) Amostra de tamanho 6000. (Figura 3.5.3)
Mensagem Fixa: E3 08 69 02 BE E4 96 3Bx
número médio de trocas esperado por iteração: 3000
número médio de trocas: 2988

Iteração	Trocas Realizadas
1	2955
2	3048
3	3048
4	2973
5	2988
6	2958
7	2967
8	2963
9	2991
10	2979
11	3041
12	2949
13	2959
14	2975
15	3026

Tabela B6: (Grupo A) Amostra de tamanho 6000. (Figura 3.5.8)
Mensagem Fixa: E3 08 69 02 BE E4 96 3Bx
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	2
2	13
3	80
4	264
5	562
6	941
7	1174
8	1194
9	885
10	540
11	256
12	70
13	17
14	2
15	0

Tabela B7: (Grupo A) Amostra de tamanho 6500. (Figura 3.5.4)
Mensagem Fixa: 23 E9 08 63 5A AF 22 93x
número médio de trocas esperado por iteração: 3250
número médio de trocas: 3256,4

Iteração	Trocas Realizadas
1	3340
2	3298
3	3345
4	3209
5	3241
6	3199
7	3247
8	3314
9	3237
10	3193
11	3204
12	3215
13	3257
14	3288
15	3259

Tabela B8: (Grupo A) Amostra de tamanho 6500. (Figura 3.5.9)
Mensagem Fixa: 23 E9 08 63 5A AF 22 93x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 15

Trocas Realizadas	Ciframentos
0	1
1	1
2	18
3	103
4	283
5	533
6	991
7	1294
8	1306
9	986
10	590
11	280
12	91
13	18
14	4
15	1

Tabela B9: (Grupo A) Amostra de tamanho 7000. (Figura 3.5.5)
Mensagem Fixa: 9E 0A 99 56 81 DD 6F F7x
número médio de trocas esperado por iteração: 3500
número médio de trocas: 3511

Iteração	Trocas Realizadas
1	3470
2	3533
3	3549
4	3511
5	3477
6	3448
7	3518
8	3497
9	3541
10	3543
11	3468
12	3509
13	3500
14	3538
15	3568

Tabela B10: (Grupo A) Amostra de tamanho 7000. (Figura 3.5.10)
Mensagem Fixa: 9E 0A 99 56 81 DD 6F F7x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	1
1	4
2	23
3	85
4	281
5	652
6	1042
7	1391
8	1348
9	1116
10	625
11	306
12	100
13	21
14	5
15	0

Tabela B11: (Grupo B) Amostra de tamanho 5000. (Figura 3.5.11)
Mensagem Fixa: 4A 21 FF 77 CA EF 15 C5x
número médio de trocas esperado por iteração: 2500
número médio de trocas: 2498,33

Iteração	Trocas Realizadas
1	2469
2	2528
3	2441
4	2473
5	2506
6	2512
7	2557
8	2433
9	2486
10	2470
11	2488
12	2506
13	2536
14	2528
15	2542

Tabela B12: (Grupo B) Amostra de tamanho 5000. (Figura 3.5.16)
Mensagem Fixa: 4A 21 FF 77 CA EF 15 C5x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	1
1	2
2	9
3	81
4	190
5	496
6	765
7	931
8	983
9	816
10	427
11	216
12	70
13	11
14	2
15	0

Tabela B13: (Grupo A) Amostra de tamanho 5500. (Figura 3.5.12)
Mensagem Fixa: CB D4 81 6A DB 7C FA A9x
número médio de trocas esperado por iteração: 2750
número médio de trocas: 2739,6

Iteração	Trocas Realizadas
1	2752
2	2734
3	2724
4	2730
5	2745
6	2689
7	2757
8	2754
9	2716
10	2759
11	2807
12	2755
13	2701
14	2764
15	2707

Tabela B14: (Grupo B) Amostra de tamanho 5500. (Figura 3.5.17)
Mensagem Fixa: CB D4 81 6A DB 7C FA A9x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 15

Trocas Realizadas	Ciframentos
0	1
1	2
2	24
3	80
4	239
5	497
6	836
7	1113
8	1063
9	848
10	475
11	220
12	79
13	21
14	1
15	1

Tabela B15: (Grupo B) Amostra de tamanho 6000. (Figura 3.5.13)
Mensagem Fixa: 2B 9E 92 93 32 28 B3 46x
número médio de trocas esperado por iteração: 3000
número médio de trocas: 3000,93

Iteração	Trocas Realizadas
1	3009
2	3016
3	3018
4	3020
5	3013
6	2970
7	3004
8	2973
9	3048
10	2935
11	3035
12	3022
13	2938
14	2998
15	3015

Tabela B16: (Grupo B) Amostra de tamanho 6000. (Figura 3.5.18)
Mensagem Fixa: 2B 9E 92 93 32 28 B3 46x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	4
2	17
3	74
4	261
5	555
6	906
7	1135
8	1228
9	924
10	560
11	240
12	77
13	16
14	3
15	0

Tabela B17: (Grupo B) Amostra de tamanho 6500. (Figura 3.5.14)
Mensagem Fixa: 6C 7F 30 F4 CD F3 3F 9Dx
número médio de trocas esperado por iteração: 3250
número médio de trocas: 3243,07

Iteração	Trocas Realizadas
1	3291
2	3243
3	3235
4	3215
5	3260
6	3212
7	3230
8	3240
9	3268
10	3290
11	3244
12	3244
13	3236
14	3207
15	3231

Tabela B18: (Grupo B) Amostra de tamanho 6500. (Figura 3.5.19)
Mensagem Fixa: 6C 7F 30 F4 CD F3 3F 9Dx
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	2
2	25
3	101
4	274
5	591
6	1030
7	1250
8	1248
9	980
10	631
11	245
12	101
13	19
14	3
15	0

Tabela B19: (Grupo B) Amostra de tamanho 7000. (Figura 3.5.15)
Mensagem Fixa: E6 A0 C2 E7 F4 21 8C 02x
número médio de trocas esperado por iteração: 3500
número médio de trocas: 3504,73

Iteração	Trocas Realizadas
1	3491
2	3517
3	3533
4	3493
5	3435
6	3537
7	3511
8	3474
9	3496
10	3526
11	3455
12	3592
13	3510
14	3553
15	3448

Tabela B20: (Grupo B) Amostra de tamanho 7000. (Figura 3.5.20)
Mensagem Fixa: E6 A0 C2 E7 F4 21 8C 02x
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	1
1	1
2	17
3	94
4	267
5	628
6	1100
7	1402
8	1358
9	1086
10	658
11	276
12	83
13	24
14	5
15	0

Tabela B21: (Grupo C) Amostra de tamanho 5000. (Figura 3.5.21)
número médio de trocas esperado por iteração: 2500
número médio de trocas: 2489,13

Iteração	Trocas Realizadas
1	2507
2	2472
3	2467
4	2499
5	2450
6	2444
7	2481
8	2519
9	2530
10	2468
11	2562
12	2449
13	2491
14	2530
15	2468

Tabela B22: (Grupo C) Amostra de tamanho 5000. (Figura 3.5.26)
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	3
2	16
3	76
4	182
5	478
6	778
7	1021
8	1007
9	711
10	432
11	200
12	83
13	12
14	1
15	0

Tabela B23: (Grupo C) Amostra de tamanho 5500. (Figura 3.5.22)
número médio de trocas esperado por iteração: 2750
número médio de trocas: 2748,27

Iteração	Trocas Realizadas
1	2742
2	2734
3	2678
4	2716
5	2731
6	2770
7	2751
8	2818
9	2775
10	2718
11	2845
12	2715
13	2717
14	2786
15	2728

Tabela B24: (Grupo C) Amostra de tamanho 5500. (Figura 3.5.27)
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 0
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	1
1	1
2	27
3	79
4	222
5	517
6	833
7	1094
8	1026
9	866
10	503
11	226
12	85
13	15
14	5
15	0

Tabela B25: (Grupo C) Amostra de tamanho 6000. (Figura 3.5.23)
número médio de trocas esperado por iteração: 3000
número médio de trocas: 3010,27

Iteração	Trocas Realizadas
1	2965
2	3022
3	3017
4	3011
5	2970
6	3013
7	3048
8	2982
9	2954
10	3008
11	2983
12	3039
13	3018
14	3046
15	3078

Tabela B26: (Grupo C) Amostra de tamanho 6000. (Figura 3.5.28)
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	2
2	18
3	89
4	228
5	567
6	921
7	1148
8	1165
9	920
10	561
11	264
12	96
13	20
14	1
15	0

Tabela B27: (Grupo C) Amostra de tamanho 6500. (Figura 3.5.24)
número médio de trocas esperado por iteração: 3250
número médio de trocas: 3235,73

Iteração	Trocas Realizadas
1	3284
2	3271
3	3232
4	3288
5	3141
6	3237
7	3240
8	3298
9	3250
10	3235
11	3255
12	3183
13	3235
14	3236
15	3151

Tabela B28: (Grupo C) Amostra de tamanho 6500. (Figura 3.5.29)
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 14

Trocas Realizadas	Ciframentos
0	0
1	2
2	21
3	87
4	275
5	647
6	1016
7	1244
8	1278
9	972
10	561
11	278
12	99
13	16
14	4
15	0

Tabela B29: (Grupo C) Amostra de tamanho 7000. (Figura 3.5.25)
número médio de trocas esperado por iteração: 3500
número médio de trocas: 3487,33

Iteração	Trocas Realizadas
1	3476
2	3424
3	3432
4	3446
5	3517
6	3530
7	3453
8	3541
9	3527
10	3474
11	3428
12	3496
13	3566
14	3530
15	3470

Tabela B30: (Grupo C) Amostra de tamanho 7000. (Figura 3.5.30)
número médio de trocas esperado por ciframento: 7
número médio de trocas: 7
número mínimo de trocas: 1
número máximo de trocas: 15

Trocas Realizadas	Ciframentos
0	0
1	4
2	20
3	108
4	305
5	655
6	1089
7	1349
8	1364
9	1038
10	670
11	286
12	91
13	17
14	3
15	1

Referências Bibliográficas

[BKPS91] Brown, L., Kwan, M., Pieprzyk, J., Seberry, J., "Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI", Proceedings of ASIACRYPT'91, 25-30, 1991.

[BM86] Brickell, E.F., Moore, J.H., Purtill, M.R."Structure in the S boxes of the DES", Lecture Notes in Computer Science 263, Advances in Cryptology, Proceedings of CRYPTO'86, 3-7, 1986.

[Bo88] Boer, B.Den, "Cryptanalysis of the F.E.A.L.", Lecture Notes in Computer Science 330, Advances in Cryptology, Proceedings of EUROCRYPT'88, 293-300, 1988.

[BP82] Becker, H., Piper, F., "Cipher Systems", John Wiley & Sons, 1982.

[BPS90] Brown, L., Pieprzyk, J., Seberry, J., "LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications", Advances in Cryptology-AUSCRYPT'90, Lecture Notes 453, 229-236, 1990.

[BS90] Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems (Extended Abstract)", Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of Crypto'90, 1990.

[BS91] Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, 4:1, 3-72, 1991.

[BS92] Biham, E., Shamir, A., "Differential Cryptanalysis of the Full 16-round DES", Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of Crypto'92, 1992.

[BSe90] Brown, L., Seberry, J., "Key Scheduling in DES Type Cryptosystems", Lecture Notes in Computer Science 453, 221-228, 1990.

[CE85] Chaum, D., Evertse, J.-H., "Cryptanalysis of DES with a Reduced Number of Rounds, Sequences of Linear Factors in Blocks", Lecture Notes in Computer Science 218, Advances in Cryptology, Proceedings of Crypto'85, 192-211, 1985.

[D82] Denning, D.E.R., "Cryptography and Data Security", Addison-Wesley Publishing Company, 1982.

[Da81] Davies, D.W., "Some Regular Properties of the 'Data Encryption Standard', Advances in Cryptology, Proceedings of Crypto'82 (presented at Crypto'81), 89-96, ed. Chaun, Rivest and Sherman, Plun Press, New York, 1983.

[DD83] Davio, M., Desmedt, Y., Fosséprez, M., Govaerts, R., Hulsbosch, J., Neutjens, P., Piret, P., Quisquater, J.-J., Vandewalle, J., Wouters, P., "Analytical Characteristics of the DES", Advances in Cryptology, Proceedings of Crypto'83, 171-202, 171-202, ed. Chaun, Plun Press, New York, 1984.

[DQ84] Desmedt, Y., Quisquater, J.-J., Davio, M., "Dependence of output on input in DES: small avalanche characteristics, Advance in Cryptology, Proceedings of Crypto'84, 359-376, Plenum Press, 1984.

[F50] Feller, W., "An Introduction to Probability Theory and Its Applications", Vol. 1, John Wiley & Sons, 1950.

[GO91] Garon, G., Outerbridge, R., "DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's", Cryptologia, XV:3, 177-193, July 1991.

[HK79] Hoffman, K., Kunze, R., "Álgebra Linear", 2ª Edição, Livros Técnicos e Científicos Editora, Rio de Janeiro, 1979.

[K81] Konheim, A.G."Cryptography: A Primer", John Wiley & Sons, 1981.

[Ka79] Kannan, D., "An Introduction to Stochastic Processes", North Holland Scientific Publishers, Ltd., 1979.

[Kn91] Knudsen, L.R. "Cryptanalysis of LOKI (Extended Abstract)" , Proceedings of ASIACRYPT'91, 19-24, 1991.

[Kn92] Knudsen, L.R."Iterative Characteristics of DES and s^2-DES", Notes in Computer Science, Advances in Cryptology, Proceedings of Crypto'92, 1992.

[KT93] Koyama, K., Terada, R., "Randomization to Strengthen DES-like Cryptosystems against Differential Cryptanalysis", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E76-A, 63-69, 1993.

[LM90] Lai, X., Massey, J.L., "A Proposal for a New Block Encryption Standard", Advances in Cryptology, Proceedings of Eurocrypt'90, 389-404, 1990.

[LM91] Lai, X., Massey, J.L., "Markov Ciphers and Differential Cryptanalysis", Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of Eurocrypt'91, 1991.

[Lu86] Lucchesi, C.L., "Introdução à Criptografia Computacional", Editora da Unicamp, 1986.

[NBS77] National Bureau of Standards, Data Encryption Standard, FIPS Publication 46, U.S. Dept. of Commerce, January (1977).

[Pf89] Pfleeger, C.P., "Security in Computing", Prentice-Hall, 1989.

[QD89] Quisquater, J.-J., Delescaille, J.-P., How easy is collision search. New Results and Applications to DES (Abstract and Results)", Lecture Notes in Computer Science 435, Advances in Cryptology, 408-413, 1989.

[QD89a] Quisquater, J.-J., Delescaille, J.-P., "How easy is collision search? Application to DES (Extended Abstract)", Lecture Notes in Computer Science 434, Advances in Cryptology, Proceedings of EUROCRYPT'89, 429-433, 1989.

[RS78] Rivest, R.L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Criptosystems", Communications of ACM, Vol.21, 120-126, 1978.

[So87] Solomon, F., "Probability and Stochastic Processes", Prentice-Hall Inc., 1987.

[Sh49] Shannon, C.E., Communication Theory of Secrecy Systems, Bell System Technical Journal, 28, 656-715, 1949.