

Um Estudo Comparativo entre algoritmos de criptografia DES – *Lucifer* (1977) e AES – *Rijndael* (2000)

Leandro Salenave Gonçalves

leandrus@ca.conex.com.br

Bel. Ciências da Computação (ULBRA 2001)

Vinicius Gadis Ribeiro

vribeiro@inf.ufrgs.br

Professor Adjunto da ULBRA e UNILASALLE*

Doutorando Computação (PPGC-UFRGS)

Membro do GSeg/UFRGS

Universidade Luterana do Brasil - Prédio 14, sala 215 (Faculdade de Informática)

Rua Miguel Tostes, 101

Bairro São Luís

CEP 92.420-280 Canoas/RS

Fone/Fax: 55- 51 - 477 4000

BRASIL

Resumo

Este artigo apresenta um estudo comparativo sobre aspectos de desempenho entre os algoritmos de criptografia *Data Encryption Standard* - DES -, e *Advanced Encryption Standard* - AES (Rijndael). Para tanto, inicialmente é apresentado o funcionamento básico de cada algoritmo; posteriormente, são definidas as variáveis que conduziram a presente experimentação - tais como o desempenho de processamento, o consumo de recursos e o tempo despendido na geração dos arquivos criptografados. Posteriormente, são apresentados os resultados do trabalho e considerações para trabalhos futuros.

Palavras-chave: Segurança Computacional, Criptografia, Criptografia de bloco, DES, AES.

Abstract

This paper presents a comparative study about performance considerations between cryptography algorithms Data Encryption Standard - DES -, e Advanced Encryption Standard - AES(Rijndael). First, it's presented the basic function of each one; after, variables are defined, to conduct this experimentation - as processing performance, resources use, and time spent in generation of cryptography files. Following, are presented the results of this study, and considerations on future works.

Keywords: *Computer Security, Cryptography, block cryptography, DES, AES.*

A criptografia está diretamente relacionada à segurança; com ela busca-se garantir que, mesmo que uma informação seja acessada por uma pessoa não-autorizada, dificilmente o conteúdo será conhecido. A criptografia é a forma mais antiga de escrevermos uma mensagem de maneira que apenas pessoas autorizadas - normalmente o emissor e o receptor - tenham conhecimento do conteúdo que está sendo transmitido. O uso da criptografia antecede o trabalho com o computador,

* Esse estudo foi parcialmente patrocinado pelo Centro Universitário LaSalle - UNILASALLE -, e pela Universidade Luterana do Brasil - ULBRA.

desde a Roma Antiga os imperadores já faziam uso destas técnicas para transmitir comandos à seus soldados, culminando sua utilização durante o período da Segunda Guerra Mundial.

Todas as técnicas de criptografia conhecida como "convencional" - ou de bloco - são derivadas da substituição e da transposição [5]. Basicamente, a substituição consiste na troca simples de um dígito ou bloco dígitos por outros. A transposição é normalmente efetuada em blocos de caracteres, onde as posições vão sendo trocadas em pares ordenados ou através de processos de arranjo, combinação o permutação. Mesmo não sendo uma técnica criptográfica, as chaves são de extrema eficiência no ato de barrar a quebra do arquivo cifrado. As chaves são agregadas ao código, buscando manter a mesma distribuição de frequência encontrada das letras dentro do texto.

O recente processo seletivo para definir o novo padrão criptográfico americano - *Advanced Encryption Standard*(AES), que passa a substituir o *Data Encryption Standard* (DES) - leva a algumas questões: que melhorias foram incorporadas no novo padrão, além de garantir se o novo padrão será melhor do que o anterior em todos os aspectos - considerando-se sobretudo os aspectos de desempenho. Buscando-se responder a essas questões, conduziu-se um estudo comparativo entre os dois algoritmos, por intermédio de uma experimentação.

A seguir, serão apresentados dados sobre os algoritmos de Criptografia Padrão de Dados - *Data Encryption Standard* (DES) e o Padrão Avançado de Criptografia - *Advanced Encryption Standard* (AES), apresentando o funcionamento de cada um e o conjunto de técnicas utilizadas até a geração do arquivo criptografado. Posteriormente, são apresentadas as condições de condução do experimento, seus resultados, e limitações e conclusões do presente trabalho.

Data Encryption Standard

O *Data Encryption Standard* – DES - é um padrão criptográfico criado em 1977 através de uma licitação aberta pela antiga Agência Nacional de Segurança americana - *National Security Agency* (NSA). O único concorrente foi o algoritmo LUCIFER da *International Business Machine* - IBM[5]. Após algumas modificações no seu código original, chegou-se ao padrão de 64 bits de leitura, aplicando uma chave com 56 bits à mensagem.

Tanto o algoritmo quanto a chave são simétricos, ou seja, são os mesmos utilizados na geração do arquivo criptografado quanto na sua descryptografia.

A estrutura do funcionamento do DES pode ser dividida em três partes: permutação inicial, cifragens com operações de chave e permutação final [1][5] [6].

As permutações iniciais e finais são processos de transposição dos blocos de entrar, executando a leitura da esquerda para direita. Já a cifragem com operações de chave é executada repetindo 16 vezes a mesma operação. Inicialmente o bloco de entrada e a chave são divididos em duas partes de mesmo tamanho, é executado processos de permutação, transformação e expansão de chave. A cada bloco executado, uma nova chave gerada.

A decifragem do DES pode ser executada no mesmo algoritmo de entrada. A única alteração fica por conta da ordem de operação. Todos processos devem ser descritos na ordem inversa da sua geração - do último para o primeiro. O esquema de funcionamento do DES encontra-se na figura 3, em anexo.

Por ser um algoritmo muito visado, inúmeros testes tentando quebrar o DES foram testados; talvez a tentativa que tenha empregado o mais espetacular recurso obteve sucesso em 1998 através da técnica conhecida por “força bruta” com a emprego de um *cluster* de computadores, tendo um *Cray* como computador mestre. Tal atividade contribuiu para reforçar na prática o conceito que já existia - graças à criptoanálise efetuada anteriormente - de uma lista de chaves que possuem uso desaconselhável, nomeadas de "fracas" e "pseudo-fracas".

Há ainda diversos trabalhos voltados à criptoanálise do DES - não citadas aqui, por fugir ao escopo do presente trabalho.

Advanced Encryption Standard

Uma disputa muito mais acirrada pode perceber-se no final milênio passado quanto à criação do novo padrão criptográfico. Durante 4 anos cientistas da computação e matemáticos do mundo disputaram pela publicação do seu algoritmo no *Advanced Encryption Standard* (AES). Os algoritmos concorrentes deveriam possuir blocos de leitura de 128 bits com chaves simétricas de 128, 192 ou 256 bits, código publicado para testes e liberação para padronizações do Instituto Nacional de Padrões e Tecnologia – *National Institute of Standard and Technology* (NIST) – caso fosse escolhido como vencedor.

O algoritmo Rijndael, dos belgas Joan Daemen e Vicente Rijmen foi eleito o vencedor do concurso obtendo maior soma de pontos votados pelos Engenheiros de Sistemas do NIST e público em geral através de cartas e correspondências manuais ou eletrônicas. Disputaram com o Rijndael: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH [2].

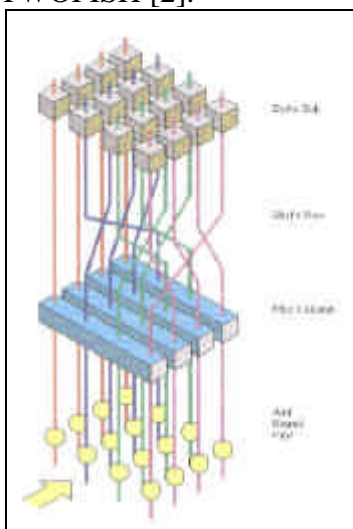


Figura 1 - O esquema do funcionamento do Rijndael.

Fonte: NIST [2]

O Rijndael opera em quatro camadas: substituição de bytes, deslocamento de linhas, mistura de colunas e adição da chave[2]. A substituição de bytes é um processamento não linear através de caixas S-Box¹. O deslocamento de linhas tem por objetivo fazer uma transposição dos blocos resultantes das caixas S-Box. A mistura de colunas é obtida através de uma fórmula matemática com o objetivo de unir diferentes colunas de forma ordenada. A adição de chaves varia conforme o tamanho indicado na criptografia, após esta execução o processamento está pronto para fechamento da criptografia e geração do arquivo de saída.

Condução do Experimento

Um estudo comparativo é a forma mais simples de se conduzir uma experimentação [4]. Uma experimentação é um dos métodos de pesquisa onde se assumem condições especiais - sob grande controle - de variáveis de interesse [3]. Essas variáveis podem ser independentes - tais como o tamanho dos arquivos, o tamanho das chaves, a composição dos arquivos ou das chaves² - ou dependentes - tal como o tempo, por exemplo.

Para poder realizar a análise comparativa, resultante da coleta de dados da execução dos algoritmos de criptografia DES e AES, fez-se necessário o desenvolvimento de um protótipo atendendo características em comum. O equipamento utilizado para tabulação dos dados foi um AMD© K6II-Pro® 333Mhz com 32MB de Memória RAM. A linguagem de programação utilizada

¹ S-BOX: Funções que recebe um conjunto de bits, reordena-os conforme uma ordem específica e os envia como saída - em suma, realizam a técnica de substituição, conforme alguma tabela ou função.

² Ou seja, se algum arquivo foi alterado - o que é de interesse para o teste de perturbação.

para descrever ambos algoritmos foi o C, em ambiente Turbo C ++® , sendo executado sob o Sistema Operacional MS-DOS® 7.0. Assim, todas as afirmações aqui realizadas se limitam a essas condições.

Para fins de se investigar questões de desempenho, foram testadas a influência do aumento no tamanho do arquivo criptografado sobre o tempo para criptografá-lo, além de se verificar o quanto um arquivo criptografado era maior do que o arquivo original. Ademais, foi identificado o quanto de memória RAM era necessário para cada algoritmo, e se o aumento do tamanho do arquivo influenciava na necessidade de maior quantidade de memória RAM.

Para se investigar a influência da alteração dos elementos de entrada - tais como a influência de pequenas alterações que os arquivos criptografados sofreram sobre os arquivos a serem criptografados e as chaves empregadas -, foram realizados testes onde se alterou apenas 1 bit do arquivo de entrada, e analisada a influência dessa alteração; posteriormente, também se alterou apenas 1 bit da chave, e novamente analisada a influência que essa alteração proporcionou. Esse procedimento é aqui referido como "Teste de Perturbação". As entradas foram executadas com arquivos texto padrão com tamanho de 1024 bytes. Empregaram-se chaves cujos conteúdos eram repetições de bits - compostos exclusivamente de 0's, ou compostos exclusivamente de 1's. Assim, pode-se melhor observar a influência da alteração de 1 bit na chave.

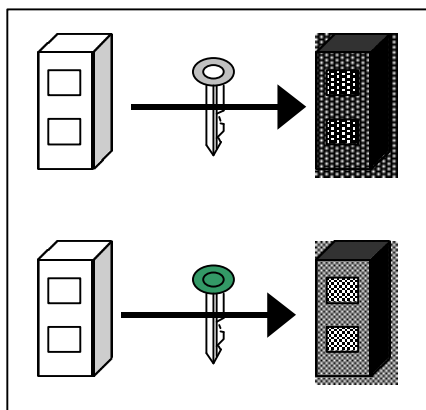


Figura 2: O teste de perturbação, considerando-se a alteração em um bit da chave.

Fonte: elaborado pelos autores, com base na pesquisa realizada.

A figura acima ilustra o procedimento experimental básico para efetuar o teste de perturbação considerando-se a alteração de um bit na chave - em ambos os algoritmos. De modo similar, procedeu-se mantendo-se a mesma chave para ambos os algoritmos, mas alterando-se um bit do arquivo original. Desejava-se, em ambos os casos, observar as alterações decorrentes da operação de criptografia.

Os detalhes das condições iniciais do experimento referiam-se ao arquivo original - o qual tinha 1.024 bytes -, contendo todos os bits originalmente setados em 0, bem como a chave empregada tinha todos os bits setados em 0.

Resultados do experimento

A seguir, são apresentadas as tabelas contendo os resultados do experimento referentes aos dados da comparação entre os algoritmos tomando como base o tempo de execução.

O item "tempo de execução" é a base para efetuar a comparação do desempenho de cada um dos algoritmos. Tomando como base os arquivos de entrada, pode-se notar que o DES é mais rápido em todos os casos que o AES. Certamente este ponto poderá ser de elevada relevância a instituições que utilizam o algoritmo DES e desejam substituí-lo pelo novo padrão criptográfico.

Ao se verificar a quantidade de memória RAM requerida para o processo de criptografia, destaca-se que o DES demonstra maior eficiência, ocupando menos recursos de máquina que o AES. Durante todo o processamento dos algoritmos DES e Rijndael, observou-se a mesma quantia

de memória alocada: o DES emprega 1024 bytes, ao passo que o Rijndael emprega 2624 bytes. Observou-se que o aumento no tamanho no arquivo não requereu o aumento proporcional de memória RAM.

Tabela 1 – Comparação do tempo de execução do algoritmo de criptografia

Tamanho em (bytes)	Tempo - DES (em s)	Tempo - Rijndael (em s)
1024	10	15
2048	17	31
3072	21	48
4096	24	58

Fonte: Elaborado pelos autores, com base na experimentação realizada.

Conforme pode-se observar na tabela 1, o Rijndael leva 50 % mais tempo que o DES, para realizar a criptografia em bloco de 1KB. Conforme esperado, o tempo para realizar a criptografia é diretamente proporcional ao tamanho do arquivo a ser criptografado. Destaca-se, contudo, que em arquivos de tamanhos maiores, o tempo decorrido é cerca do dobro do tempo que o DES leva. Em outras palavras, nas condições em que foi conduzido o experimento, o DES tem um desempenho melhor do que o Rijndael - se considerarmos o mesmo trabalho (criptografar um mesmo arquivo) por unidade de tempo.

Uma das questões se referia a quanto um arquivo aumentaria de tamanho, ao ser criptografado pelos dois algoritmos. A tabela que se segue apresenta os resultados obtidos.

Tabela 2 – Comparação do tamanho resultante dos arquivos (em KB)

Tamanho original do arquivo (em bytes)	Tamanho do arquivo gerado pelo DES	Tamanho do arquivo gerado pelo AES
1024	1024	2453
2048	2048	4942
3072	3072	7413
4096	4096	9884

Fonte: Elaborado pelos autores, com base na experimentação realizada.

O arquivo gerado pelo DES mantém o seu tamanho inalterado em relação ao arquivo original, ao passo que o Rijndael aumenta o arquivo em cerca de 140% a mais do que o original. Em caso de limitação de espaço em disco, essa situação coloca o Rijndael em situação inferior a do DES.

Uma questão de grande preocupação na Criptografia de Bloco é a possibilidade de ocorrência de padrões repetidos. Assim, o programa que efetuou a comparação realizou também a busca por padrões repetidos, em blocos de 4, 8 e 16 bits. Nesse caso, observa-se que o Rijndael é muito melhor do que o DES, pois possui um percentual bem menor de padrões repetidos, o que garante uma menor probabilidade de quebra do arquivo cifrado pela análise de repetições.

O primeiro experimento do teste de perturbação previa a alteração de 1 bit no arquivo original: assim, o arquivo original foi criptografado, gerando um arquivo criptografado 1; o primeiro bit do arquivo original foi setado em 1, mantendo-se todos os outros em 0, e foi criptografado, vindo a gerar um arquivo criptografado 2. Já o segundo experimento do teste de perturbação previa a alteração de 1 bit na chave original, e a conseqüente criptografia de um mesmo arquivo original, com ambas as chaves.

Esse experimento causou duas situações: a original, ou "situação de controle", e a situação onde se buscou causar alguma alteração. Assim, bastou observar os efeitos causados nos arquivos.

Comparando-se os novos arquivos criptografados nas situações 1 e 2, obtiveram-se os seguintes resultados, conforme a tabela a seguir.

Tabela 3 - Resultados do teste de perturbação pela alteração de elementos de entrada

Situação 1		Situação 2		% de bits perturbados	
Arquivo	Chave	Arquivo	Chave	DES	Rijndael
0	0	0	0p	43,42	86,50
0	0	0p	0	45,67	70,00
d	0	d	0p	46,44	75,50
d	0	dp	0	50,96	70,00
Caso médio				46,62	75,50

Fonte: elaborado pelos autores, com base na experimentação realizada.

Observam-se as seguintes legendas, para a referida tabela:

0 - elemento composto totalmente de 0s;

0p - elemento cujo primeiro componente é 1, e todos os restantes em 0 - ou seja, no caso da chave, apenas o 1º bit foi alterado, bem como no caso do arquivo;

d - string de dados composta por 0..9A..Za..z, repetidamente;

dp - string de dados similar a anterior, mas o 1º bit por alterado ou seja, no caso da chave, apenas o 1º bit foi alterado, bem como no caso do arquivo.

% de bits perturbados - a quantidade de bits, em %, que foram alterados da situação 1 para a situação 2.

Os resultados variaram bastante, vista a grande variação no percentual dos bits perturbados: o algoritmo DES obteve a sua maior variação na situação onde o arquivo era composto apenas de cadeia de caracteres repetidos, os quais eram basicamente compostos por "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz", assim como a chave, e perturbou-se o 1º bit desse arquivo. No caso do Rijndael, a situação onde houve grande percentual de perturbação ocorreu quando todos os bits se encontraram em 0, e um bit da chave foi alterado.

Contudo, dadas as condições do experimento realizado, observou-se que sempre o Rijndael obteve melhor resultado do que o DES - tendo alcançado um percentual de perturbação maior do que o DES de 37,3% (onde o DES obteve 50,96%, e o Rijndael, 70,00%), até 99,2 % (onde o DES obteve 43,42%, e o Rijndael, 86,50%)

Limitações do presente estudo, conclusões e trabalhos futuros

A principal limitação do presente trabalho reside no fato de se efetuar a comparação entre um algoritmo que já constitui um padrão - DES - e uma proposta de substituição - Rijndael, o qual pode ainda sofrer alterações, no intuito de tornar-se um padrão de fato³. Ressalta-se ainda que esse último ainda concorre ao padrão europeu de criptografia - novo concurso para definir um padrão criptográfico aplicável a toda a União Européia. Do ponto de vista do referencial teórico, encontra-se vasta bibliografia acadêmica sobre o DES, mas nenhuma publicação acadêmica relevante sobre o Rijndael - excetuando-se os relatórios técnicos do conteste, e as páginas do NIST.

Em situação real, os arquivos teriam composição diferente, e as chaves não seriam as empregadas aqui. Contudo, para melhor controle - condição importante para qualquer experimentação -, foram empregados os elementos na forma explicitadas: emprego de chaves e arquivo simples, contendo pouca variação. Todas as afirmações referem-se a essas condições.

Em determinadas circunstâncias - diferente do que era esperado -, pode-se afirmar que o algoritmo do DES apresentou melhor desempenho, como nos itens tamanho do arquivo gerado (menor tamanho gerado), e tempo para executar o algoritmo (foi computado menos tempo do que o Rijndael).

³ A exemplo do que ocorreu com o *Lucifer*, ao tornar-se DES.

O Rijndael apresentou mais perturbação do que o DES. Com relação à criptografia, observa-se que o Rijndael permite um maior "embaralhamento" dos blocos, vindo a obter um maior índice de perturbação do que o DES - tanto para o caso de alterar-se bits em arquivos, quanto ao se alterar bits na chave empregada. Essa característica pode assegurar maior confiabilidade a um usuário.

Diferente do que era esperado, o fato de se aumentar o tamanho da chave ou o tamanho do arquivo não influenciou o tempo para efetuar as operações - assim, não se constituíram em funções diretamente relacionadas. Para ambos os algoritmos, a quantidade de memória RAM necessária manteve-se constante para cada um, indiferente ao tamanho do arquivo. Contudo, o Rijndael necessita mais do que o dobro dessa quantidade de memória (1,5625 vezes além o que o DES necessita).

Dentre os trabalhos futuros, incluem-se estudos referentes a criptoanálise - que fugiram do escopo do presente trabalho -, os quais podem levantar outros fatos e dados sobre os algoritmos envolvidos.

As observações contidas no presente trabalho permitem que um usuário possa escolher qual algoritmo utilizar, em função de suas limitações de hardware - podendo até haver casos onde o DES possa ser empregado, desconsiderando-se o emprego de suas já conhecidas chaves fracas e potencialmente fracas.

Bibliografia

- [1] NICHOLS, Randall K. **ICSA guide to Cryptography**. New York: McGraw-Hill, 1999. 840 p. il.
- [2] NIST, National Institute of Standards and Technology. **Advanced Encryption Standard**. Gaithersburg, 2000.
Disponível em: <<http://www.nist.gov/aes.htm>> Acesso em 25 de abril de 2001.
- [3] RIBEIRO, Vinicius Gadis. **Um estudo sobre métodos de pesquisa utilizados em segurança computacional – criptografia**. Porto Alegre: PPGC da UFRGS, 2000. 70 p. (TI 916). il.
Disponível na área de download em:
<<http://www.sinpro-rs.org.br/vinicius.gadis.ribeiro>>
- [4] SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. **Metodología de la Investigación**. México: McGraw-Hill, 1991. 514 p. il.
- [5] SCHNEIER, Bruce. **Applied Cryptography – Protocols, Algorithms and Source code in C**. 2nd ed. New York: John Wiley, 1994. 624 p. il.
- [6] STALLINGS, William. **Cryptography and network security: principles and practice**. 2nd ed. Upper Saddle River: Prentice-Hall, 1998. 574 p. il.

ANEXO

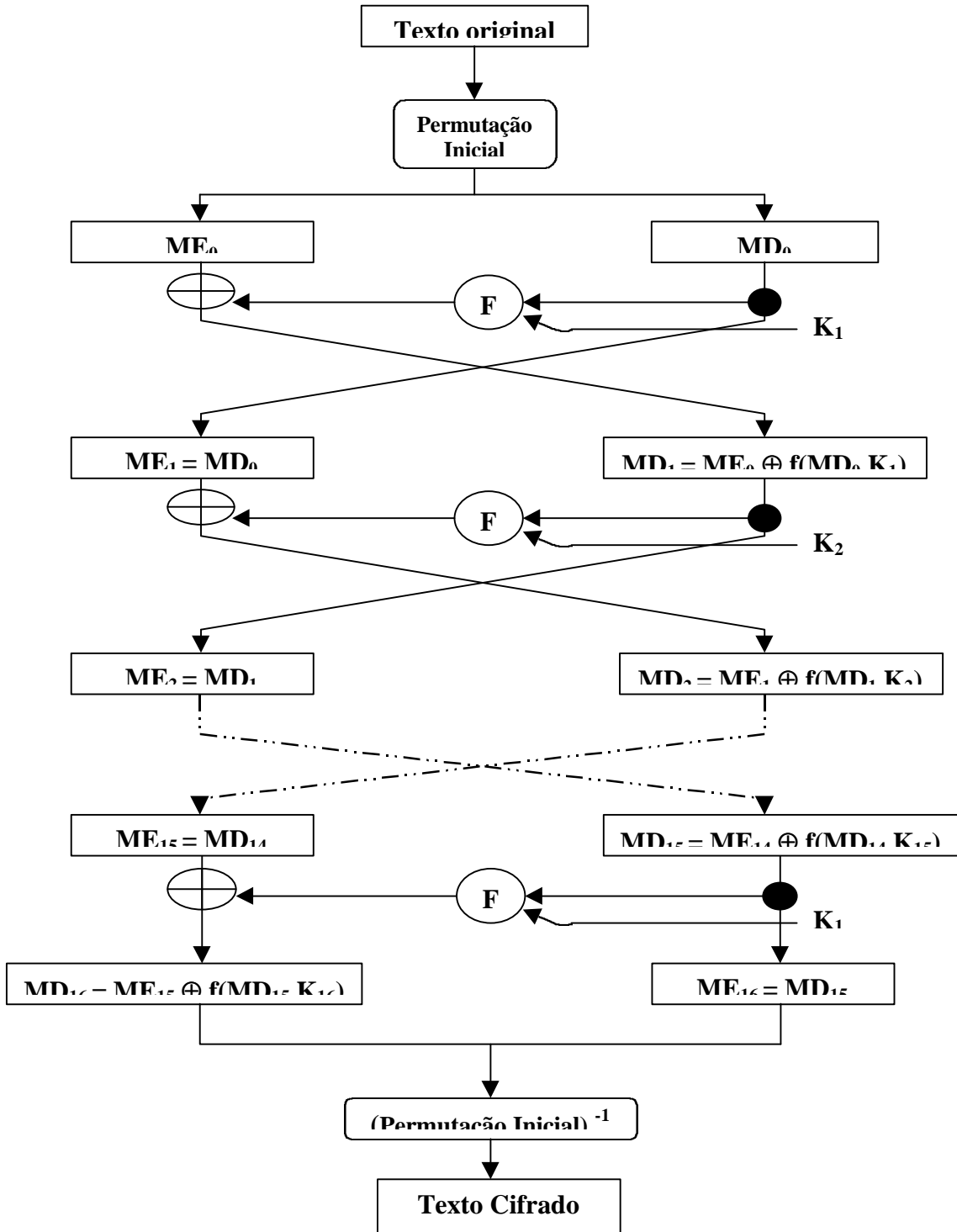


Figura 3: Esquema do funcionamento do DES.
 Fonte: Traduzido de Schneier [5].