DES - Noções Fortes de Segurança - InfoSec

Revisão

- Cifra de blocos: mensagem é transmitida e encriptada em blocos de tamanho fixo
- Instância do conceito de função/permutação aleatória
- Modos de operação de cifra de blocos: ECB, CBC etc.

Cifra de blocos iterada

- Atuação em múltiplos turnos
- Chave original k é expandida para o número de turnos que a cifra iterada usa

Cifra de Feistel: cifra iterada básica

Require: T: $2t$ bits de texto em claro
Require: $k_1, \ldots, k_R$: R chaves
Require: f: função de 1 turno da cifra com bloco de t bits
Ensure: C: $2t$ bits de texto cifrado

$E_0 \leftarrow T >> t$ ▷ $E_{0\ldots R}$ e $D_{0\ldots R}$ têm t bits cada
$D_0 \leftarrow T$ & $0xFFFF$
for r=1 ... R **do**
    $E_r \leftarrow R_{r-1}$
    $D_r \leftarrow E_{r-1} \oplus f(D_{r-1}, k_r)$
end for
return $C \leftarrow (D_R <<\text{t})\&(L_R)$ ▷ Troca direita pela esquerda

Ataque de força bruta contra o DES

- Temos pares (m_i, c_i) tal que $c_i = E(k, m_i)$ e queremos achar k
- Para um par (m, c) existe zero ou uma chave k tal que $c = E(k, m)$ com prob. $\geq 1 - 1/256 \approx 0.996$
- Se temos dois pares (m_1, c_1) e (m_2, c_2), probabilidade de k ser única é $1 - 1/2^{71}$

Desafio contra DES (RSA)

- Disponível:
  - $m =$ "The unknown messages is:" XXXXXXXXXX
  - c_i
- Meta: achar k
- Soluções:
  - Sistema distribuído: 39 dias (1998),
  - EFF máquina específica: 56 horas (1998)
  - Híbrido: 22 horas (1998)

Algoritmos de blocos atuais

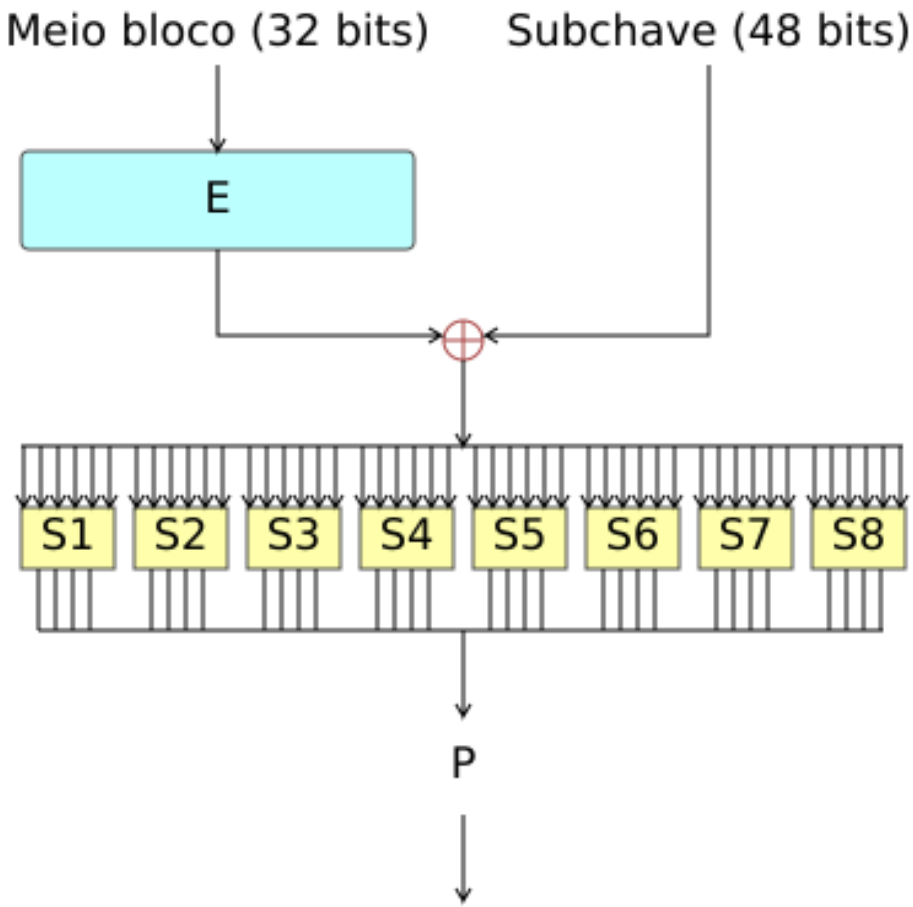
- DESX: $EX((k_1, k_2, k_3), m) = k_1 \oplus E(k_2, m \oplus k_3)$
  - Chaves: 64, 56, 64 bits
- 3DES
  - $3DES((k_1, k_2, k_3), m) = E(k_1, D(k_2, E(k_3, m)))$
  - Rede de funções Feistel: 48 turnos
  - Bloco: 64 bits. Chave: 168 bits
- AES (Advanced Encryption Standard) – Rijndael (1998)
  - Rede de substituição e transposição: 10 turnos (128 bits)
  - Bloco: 128 bits. Chave: 128, 192, 256 bits

Observação 2DES

- Ataque "Meet in the middle": $E(k_1, m) = D(k_2, m)$
- Coletar $M = (m_0, m_1, \ldots)$ e $C = (c_0, c_1, \ldots)$
- Para cada $m \in M$, construir tabela ordenada com $E(k_1, m)$ para todo valor $k_1 \in K$
- Para cada c e $k_2 \in K$, procurar $D(k_2, c)$ na tabela
- Se achou $D(k_2, c)$ então, $E(k_1, m) = D(k_2, m)$ e portanto achou as chaves!
- Custo espaço: tabela com 2^{56} posições
- Custo tempo 1: 2^{56} operações de $E(\cdot)$ e $2^{56} \log(2^{56})$ operações para ordenar
- Custo tempo 2: 2^{56} operações de $D(\cdot)$ e $2^{56} \times \log(2^{56})$ operações de busca
- Custo tempo total $< 2^{63}$

Cifra DES (Data Encryption Standard)

- Proposta pela IBM, modificada pela NSA
- Padrão FIPS PUB 46 baixar PDF
- Cifra de Feitel de 16 turnos
- Tamanho de bloco: 64 bits
- Tamanho da chave: 56 bits



Cifra de Feistel: DES

Require: T: 64 bits de texto em claro
Require: $k_1, \ldots, k_16$: chaves de 48 bits criadas de chave de 56 bits
Require: f: função de 1 turno da cifra
Ensure: C: 64 bits de texto cifrado

$T \leftarrow IP(T)$ ▷ Permutação inicial
$E_0 \leftarrow T >> 32$ ▷ $E_{0\ldots R}$ e $D_{0\ldots R}$ têm 32 bits cada
$D_0 \leftarrow T$ & $0xFFFF$
for r=1 ... R **do**
    $E_r \leftarrow R_{r-1}$
    $D_r \leftarrow E_{r-1} \oplus f(D_{r-1}, k_r)$
end for
$C \leftarrow (D_R << 32)\&(L_R)$ ▷ Troca direita pela esquerda
return $FP(C)$ ▷ Permutação final

A função de turno

Require: R: bloco de dados com 32 bits
Require: k: chave do turno com 48 bits
Require: E: função de expansão e permutação
Require: P: permutação de turno
Require: $s()$: função "caixa" S (criptografia)
Ensure: bloco de 32 bits: $R' = f(R, k)$

$X \leftarrow E(R)$ ▷ Expansão e permutação. Obtém 48 bits
$X' \leftarrow X \oplus k$
$R \leftarrow s(X')$ ▷ Aplica função não linear S e obtém 32 bits
return $P(R)$ ▷ Permutação de turno

Função "caixa" S

Require: X: 48 bits de dados

Require: $S_1, S_2, \ldots, S_8$: caixas S - tabelas de 4×16 posições de 4 bits

Ensure: bloco de 32 bits: $X' = S(X)$

$(X_1, X_2, \ldots, X_8) \leftarrow X$ ▷ Organiza X em 8 partes de 6 bits

for $i = 1 \ldots 8$ **do** ▷ Faz $X' \leftarrow (S_1(X_1), \ldots, S_8(X_8))$

$r \leftarrow 2X_i[0] + X_i[5]$

$c \leftarrow 8X_i[1] + 4X_i[2] + 2X_i[2] + X_i[3]$

$X'_i = S_i[r][c]$

end for

return X'

Exemplo de tabela da "caixa" S

- Look-up table para S_5

Índices	**0000**	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Funções auxiliares: $IP(\cdot)$, $FP(\cdot) = FP^{-1}(\cdot)$, $E(\cdot)$

- Permutação inicial $IP(\cdot)$: implementado como vetor de consulta usado para permutar bits
  - $58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4, \ldots$
  - Primeiro bit de saída é o bit 58 de entrada, ...
- Permutação final $FP(\cdot) = IP^{-1}(\cdot)$
  - $40, 8, 48, 16, 56, 24, 64, 32, 39, 7, 47, 15, 55, 23, 63, 31, \ldots$
- Função de Permutação e Expansão $E(\cdot)$:
  - $32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9 \ldots$,
  - Bits são duplicados (ver o 5) então expande de 32 para 48 bits
- Permutação de turno $P(\cdot)$:
  - $16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, \ldots$

Processamento e expansão de chave

- A chave dos DES é composta de 56 bits de chave e 8 bits de paridade
- Primeiro passo: selecionar 56 bits com
  - Tabelas de consultas "Permuted choice 1"
    - Esquerda: $57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18, \ldots$
    - Direita: $63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, \ldots$
    - Bits 8, 16, 24, 32, 40, 48, 56, 64 são de paridade
- Gerar 16 subchaves pela repetida aplicação de "Permuted choice 2" nos 56 bits de chave com descolamentos à esquerda
  - PC2: $14, 17, 11, 24, 1, 5, \ldots$
  - Descolamentos: $1, 1, 2, 2, 2, 2, 2, 2, 1, \ldots$

Exemplos de uso do DES em Java

- Ver `http://www.facom.ufu.br/~albertini/infosec/Imagem.java`
- Usar `http://www.facom.ufu.br/~albertini/infosec/tux.pnm`

3DES

- Número de turnos de funções Feistel: 48
- Tamanho do bloco: 64 bits
- Tamanho da chave: 168 bits