Cifras de Chaves Simétricas

Definição (Cifra de Chaves Simétricas)

Considere uma cifra constituída por um conjunto de funções de encriptação e desencriptação, respectivamente $\{E_e : e \in \mathcal{K}\}$ *e* $\{D_d : d \in \mathcal{K}\}$*, onde* $\mathcal{K}$ *é o espaço das chaves.*

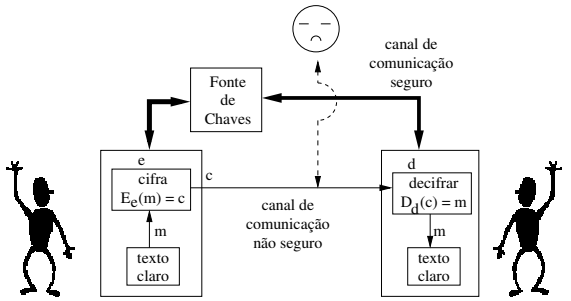
A cifra é dita uma cifra de chaves simétricas *se para cada par de chaves* (e, d)*, é computacionalmente "fácil" determinar* d *sabendo só o valor de* e *e, de igual modo, determinar* e *de* d*.*

Em muitas aplicações as chaves são iguais, $e = d$. Outros termos usados são *chave única*, *chave secreta*.

Cifras de Chaves Simétricas

Num sistema de cifra de chaves simétricas é necessário que os intervenientes tenham conhecimento das chaves simétricas (eventualmente uma só chave secreta).

A chave tem de ser enviada por um canal seguro.



Cifras de Chaves Simétricas por Blocos

As *cifras de chaves simétricas por blocos* são dos elementos mais proeminentes e importantes em muitos sistemas criptográficos.

Individualmente providenciam confidencialidade.

Como um bloco de um sistema maior a sua enorme versatilidade torna possível a construção de geradores pseudo-aleatórios, cifras fieira, MACs, e funções de dispersão.

Podem ser ainda uma das principais componentes em sistemas de autenticação de mensagens, integridade dos dados, autenticação de entidades, e esquemas de assinaturas digitais.

Cifras de Chaves Simétricas por Blocos

Não existem cifras de chaves simétricas por blocos que sejam aplicáveis a todas as situações, tal facto deve-se a:

- restrições impostas na velocidade de processamento e/ou na memória usada.
- restrições impostas pelo tipo de plataforma a ser usada (hardware e/ou software).
- diferentes níveis de tolerância das cifras a diferentes modos de utilização.

De uma forma geral às preocupações com a eficiência contrapõem-se as questões de segurança.

Cifras de Chaves Simétricas por Blocos

De entre as cifras deste tipo mais importantes temos:

- *DES* "**D**ata **E**ncryption **S**tandard", é (era!?) um das cifras deste tipo mais importantes. Estabeleceu o precedente em meados de 1970 como a primeira cifra de nível comercial com uma completa e aberta especificação dos detalhes de implementação.
- *FEAL* "**F**ast Data **E**ncipherment **Al**gorithm", é uma família de algoritmos que tiveram muita importância no desenvolvimento e melhoramento de várias técnicas de cripto-análise, nomeadamente a cripto-análise linear e diferencial.
- *AES (Rijndael)* "**A**dvanced **E**ncryption **S**tandard", foi o resultado de um esforço americano (1999) para a substituição do DES que entretanto começou a mostrar-se insuficientemente seguro.

Outras cifras deste tipo também importantes são: **IDEA** (International Data Encryption Algorithm) e **RC6**.

Cifras de Chaves Simétricas por Blocos

As cifras de chaves simétricas por blocos estão relacionadas com dois princípios gerais: cifras produto e cifras Feistel. Cada um destes princípios envolve a iteração de uma sequência comum (ou rodada) de operações.

A ideia básica de uma cifra produto é a de construir uma função de encriptação complexa por composição de várias operações simples, que embora de forma individualmente não oferecem protecção suficiente, são complementares quando combinadas podendo providenciar o grau de protecção que se deseja.
As operações básicas incluem: transposições, translações (i.e. XOR), transformações lineares ($ax + b$), multiplicação modular, e substituições simples.

Cifra Produto & Rede de Substituição-Permutação

Definição (Cifra Produto)

Uma cifra produto *combina duas ou mais transformações de tal forma que a cifra resultante seja mais segura que as componentes individuais.*

Definição (Rede de Substituição-Permutação)

Uma Rede de Substituição-Permutação *é uma cifra produto composta de um número de estágios, cada um envolvendo substituições e permutações.*

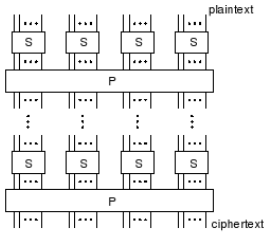


Figure 7.7: *Substitution-permutation (SP) network.*

Cifra de Blocos Iterada

Definição (Cifra de Blocos Iterada)

Uma cifra de blocos iterada *é uma cifra de blocos envolvendo a repetição sequencial de uma função interna, designada por função rodada.*
Os parâmetros de configuração da cifra incluem: o número de rodadas r, o comprimento em bits do bloco n, o comprimento em bits k, da chave de entrada K da qual r sub-chaves K_i (chaves das rodadas) são derivadas.
Por razões de invertibilidade (para permitir uma decifração única), para cada um dos valores K_i a função de rodada é uma bijecção nos valores de entrada da rodada.

Cifra Feistel

Definição (Cifra Feistel)

Uma cifra Feistel *é uma cifra de blocos iterada que aplica um texto claro de* $2t$*-bits* (L_0R_0)*, sendo que* L_0 *e* R_0 *são blocos com* t *bits, num texto cifrado* (R_rL_r)*, através de um processo com* r *rodadas, aonde* $r \geq 1$*.*

Para $1 \leq i \leq r$*, a rodada* i *aplica* $(L_{i-1}R_{i-1}) \xrightarrow{K_i} (L_iR_i)$ *da seguinte forma:* $L_i = R_{i-1}$*,* $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$*, aonde cada uma das sub-chaves* K_i *é derivada da chave da cifra* K*.*

Cifra Feistel

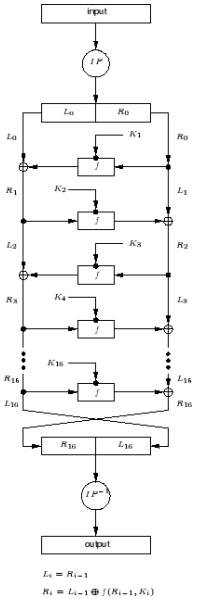
Usualmente uma cifra Feistel tem $r \geq 3$, sendo r, em geral, par.

A estrutura de uma cifra Feistel especifica a ordenação dos textos cifrados de saída com (R_rL_r) e não (L_rR_r); os blocos são trocados da sua ordenação após a última rodada.

A desencriptação é feita através do mesmo processo com r rodadas mas com a sub-chaves usadas por ordem inversa; por exemplo o último passo é desfeito através de uma simples repetição do mesmo.

A função f da cifra de Feistel pode ser uma cifra produto, no entanto a função f não necessita de ser invertível para que se possa inverter a cifra de Feistel.

Cifra Feistel



FEAL

A cifra "**F**ast Data **E**ncipherment **Al**gorithm (FEAL)" é uma família de algoritmos que têm tido um papel importante no desenvolvimento e refinamento de vários avanços nas técnicas de cripto-análise, incluindo a cripto-análise linear e diferencial.

FEAL-N aplica um texto claro de 64 bits num texto cifrado de 64 bits através de uma chave secreta de 64 bits. É uma cifra Feistel com N rodadas similar à cifra DES, mas com uma função f bastante mais simples, e aumentado por estágios iniciais e finais os quais fazem o XOR das duas metades da informação assim como o XOR das sub-chaves directamente com as metades da informação.

FEAL

FEAL foi concebido tendo em vista a velocidade e simplicidade, em especial para uma implementação de software em processadores de 8 bits (por exemplo, "chips" de cartões).

Usa operações "byte-oriented" (adições 8 bit módulo 256, rotações de dois bits para a esquerda, e XOR), evitando permutações de bits e procuras em tabelas, permitindo implementações com uma dimensão do código pequena.

A versão comercial inicialmente proposta com 4 rodadas (FEAL-4), posicionada como uma alternativa rápida ao DES, verificou-se no entanto ser consideravelmente menos segura do que se esperava.

FEAL

Verificou-se também que FEAL-8 oferecia muito menos segurança do que se pensava.

FEAL-16 ou FEAL-32 podem ainda oferecer uma segurança comparável ao DES, mas o débito da cifra reduz-se com o aumento do número de rodadas.

Além disso, enquanto a velocidade das implementações do DES pode ser melhorada através da utilização de tabelas de procura de grande dimensão, isso é mais difícil de obter com o FEAL.

Funções f

O algoritmo abaixo especifica a cifra FEAL-8. A função $f(A, Y)$ aplica um par de entrada de (32,16) bits numa saída de 32 bits. Na função f, duas substituições orientadas ao "byte" (caixas S) S_0 e S_1 são usadas, cada uma, duas vezes; sendo que cada uma delas aplica um par de entrada de 8 bits a uma saída de 8 bits.

S_0 e S_1 adicionam um único bit $d \in \{0, 1\}$ aos argumentos x e y de 8 bits, ignoram o transporte no último bit, rodam o resultado de dois bits para a esquerda (ROT2):

$$S_d(x, y) = \mathrm{ROT2}(x + y + d \bmod 256)$$

Sub-Chaves

A criação e ordenação das sub-chaves usa a função $f_K(A, B)$ similar à função f, aplicando duas entradas de 32 bits numa saída de 32 bits.

	$U \leftarrow f(A, Y)$	$U \leftarrow f_k(A, B)$
$t_1 =$	$(A_0 \oplus A_1) \oplus Y_0)$	$A_0 \oplus A_1$
$t_2 =$	$(A_2 \oplus A_3) \oplus Y_1)$	$A_2 \oplus A_3$
$U_1 =$	$S_1(t_1, t_2)$	$S_1(t_1, t_2 \oplus B_0)$
$U_2 =$	$S_0(t_2, U_1)$	$S_0(t_2, U_1 \oplus B_1)$
$U_0 =$	$S_0(A_0, U_1)$	$S_0(A_0, U_1 \oplus B_2)$
$U_3 =$	$S_1(A_3, U_2)$	$S_1(A_3, U_2 \oplus B_3)$

Figura: Saída: $U = (U_0 U_1 U_2 U_3)$ para as funções FEAL f e f_K

A_i, B_i, Y_i, t_i, e U_i são variáveis de 8 bits.

Algoritmo FEAL

Algoritmo FEAL-8

ENTRADA: texto claro de 64 bits $M = m_1 \dots m_{64}$; chave de 64 bits $K = k_1 \dots k_{64}$
SAÍDA: texto cifrado de 64 bits $C = c_1 \dots c_{64}$.

1. Calcular dezasseis sub-chaves de 16 bits K_i a partir de K.
2. Definir $M_L = m_1 \dots m_{32}$, $M_R = m_{33} \dots m_{64}$.
3. $(L_0 R_0) \leftarrow (M_L M_R) \oplus ((K_8 K_9)(K_{10} K_{11}))$, XOR com o penúltimo grupo de quatro sub-chaves (8 a 11).
4. $R_0 \leftarrow R_0 \oplus L_0$.

Algoritmo FEAL (continuação)

Algoritmo FEAL-8 (continuação)

5. Para i de 1 a 8 faz:
   1. $L_i \leftarrow R_{i-1}$
   2. $R_i \leftarrow L_{i-1} \oplus f(R_{i-1}, K_{i-1})$.

   Usando a tabela apropriada para a obtenção de $f(A, Y)$ com $A = R_{i-1} = (A_0 A_1 A_2 A_3)$ e $Y = K_{i-1} = (Y_0 Y_1)$.
6. $L_8 \leftarrow L_8 \oplus R_8$.
7. $(R_8 L_8) \leftarrow (R_8 L_8) \oplus ((K_{12} K_{13})(K_{14} K_{15}))$. XOR com o último grupo de quatro sub-chaves (12 a 15).
8. $C \leftarrow (R_8 L_8)$. A ordem final dos blocos é trocada.

Determinação das Sub-chaves

FEAL-8: Determinação das Sub-chaves

ENTRADA: Chave de 64 bits, $K = k_1 \dots k_{64}$.
SAÍDA: Chave estendida de 256 bits (16 sub-chaves de 16 bits K_i, $0 \leq i \leq 15$).

1. Inicialização:
   $U^{(-2)} \leftarrow 0$, $U^{(-1)} \leftarrow k_1 \dots k_{32}$, $U^{(0)} \leftarrow k_{33} \dots k_{64}$.
2. Calcular $K_0, \dots, K_{15}$ com i de 1 a 8:
   1. $U \leftarrow f_K(U^{(i-2)}, U^{(i-1)} \oplus U^{(i-3)})$.
   2. $K_{2i-2} = (U_0 U_1)$, $K_{2i-1} = (U_2 U_3)$, $U^{(i)} \leftarrow U$.

Com f_K definida pela tabela apropriada, aonde A e B denotam vectores de 4 "bytes": $A = U^{(i-2)} = (A_0 A_1 A_2 A_3)$;
$B = U^{(i-1)} \oplus U^{(i-3)} = (B_0 B_1 B_2 B_3)$.
Com $U \stackrel{\text{def}}{=} (U_0 U_1 U_2 U_3)$ para U_i com 8 bits.

Desencriptação & Generalizações

Nota (FEAL, Desencriptação)

A desencriptação da cifra FEAL pode se obtida usando o mesmo algoritmo, com a mesma chave e texto cifrado $C = (R_8, L_8)$ como texto claro de entrada M, mas com a ordem das sub-chaves trocada. Mais especificamente, as sub-chaves $((K_{12} K_{13})(K_{14} K_{15}))$ são usadas no XOR inicial, as sub-chaves $((K_8 K_9)(K_{10} K_{11}))$ para o XOR final, e as chaves de rodada são dadas por K_7 até K_0. Isto é análogo à desencriptação da cifra DES.

Nota (FEAL-N)

A cifra FEAL com chave de 64 bits pode ser generalizado para N rodadas, com N par. recomenda-se a utilização de um $N = 2^x$, para $x = 3$ tem-se FEAL-8. FEAL-N usa $N + 8$ sub-chaves de 16 bits: $K_0, \dots, K_{N-1}$, nas rodadas $0 \leq 1 \leq n - 1$; $K_N, \dots, K_{N+3}$ para o XOR inicial; e $K_{N+4}, \dots, K_{N+7}$ para o XOR final.
O algoritmo de determinação das sub-chaves é generalizado para calcular as sub-chaves K_0 até K_{N+7}, com $1 \leq i \leq (N/2) + 4$.

Generalizações

Nota (FEAL-NX)

A extensão da cifra FEAL-N para a utilização de chaves com 128 bits é designada por FEAL-NX. A extensão é feita da seguinte forma:

- *A chave é dividida em duas metades de 64 bits* $(K_L K_R)$.
- K_R *é dividida em duas metades de 32 bits* $(K_{R_1} K_{R_2})$.
  - *para* $1 \leq 1 \leq (N/2) + 4$, *define-se* $Q_i = K_{R_1} \oplus K_{R_2}$ *para* $i \equiv 1 \mod 3$; $Q_i = K_{R_1}$ *para* $i \equiv 2 \mod 3$; *e* $Q_i = K_{R_2}$ *para* $i \equiv 0 \mod 3$.
  - *O segundo argumento* $(U^{(i-1)} \oplus U^{(i-3)})$ *de* f_K *no passo 2.1 do algoritmo de determinação das sub-chaves é substituído por* $U^{(i-1)} \oplus U^{(i-3)} \oplus Q_i$.

Para $K_R = 0$, *FEAL-NX é igual a igual a FEAL-N com* K_L *a chave de 64 bits* K.

Exemplo

Exemplo

Para (em hexadecimal) um texto claro $M = 00000000\ 00000000$ e chave $K = 01234567\ 89ABCDEF$, o algoritmo de geração das sub-chaves gera as chaves
$(K_0, \ldots, K_7) =$
$DF3BCA36\ F17C1AEC\ 45A5B9C7\ 26EBAD25$,
$(K_8, \ldots, K_{15}) =$
$8B2AECB7\ AC509D4C\ 22CD479B\ A8D50CB5$.
O algoritmo FEAL-8 gera o texto cifrado
$C = CEEF2C86\ F2490752$.
Para FEAL-16, o correspondente texto cifrado é
$C = 3ADE0D2A\ D84D0B6F$.
Para FEAL-32 $C = 69B0FAE6\ DDED6B0B$.
Para uma chave de 128 bits (K_L, K_R) com $K_L = K_R = K$ como se viu acima, M tem com texto cifrado FEAL-8X correspondente $C = 92BEB65D\ 0E9382FB$.

Crito-análise

Cripto-análise das Cifras Fiestel.

M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - EUROCRYPT'93 (LNCS no. 765), Springer-Verlag, pp. 386-397, 1994.

E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

Howard M. Heys, *A Tutorial on Linear and Differential Cryptanalysis*, Memorial University of Newfoundland, Canada, (Internet)

Cripto-análise Linear

A cripto-análise linear explora a alta probabilidade de ocorrência de expressões lineares envolvendo bits do texto claro, do texto cifrado, e das sub-chaves.

- É um **ataque texto claro conhecido**:
  - o atacante tem à sua disposição um conjunto de textos claros e os correspondentes textos cifrados.
  - o atacante não tem forma de seleccionar os textos claros (e os correspondentes textos cifrados) a que tem acesso.

Cripto-análise Linear

A ideia base é a de aproximar uma porção da cifra com uma expressão linear, sendo que a linearidade se refere a uma operação de bits, módulo 2.
Um tal expressão é da forma:

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

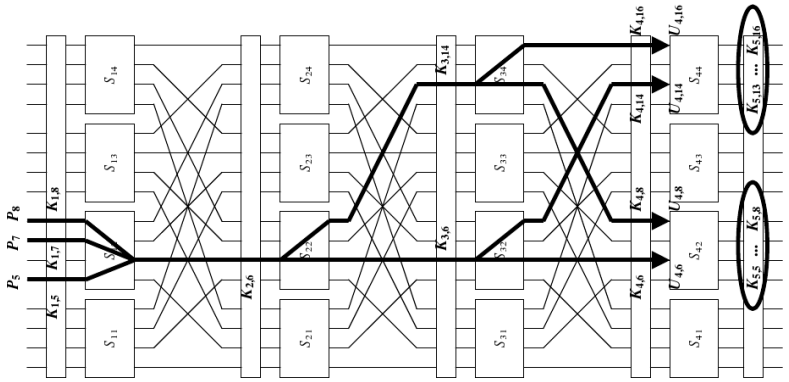
aonde X_i representa o bit de ordem i da entrada $X = [X_1, X_2, \ldots]$ e Y_j representa o bit de ordem j da saída $Y = [Y_1, Y_2, \ldots]$.

A aproximação na cripto-análise linear é a de determinar expressões da forma referida acima que tenham uma alta, ou baixa, probabilidade de ocorrência.

Considerando que num caso em que os valores escolhidos são aleatórios, a probabilidade da ocorrência de uma tal expressão é de, exactamente, $1/2$.

É o desvio, em relação ao valor de $1/2$, para a ocorrência de uma tal expressão, que é explorado na cripto-análise linear.

Cripto-análise Linear



Resistência à Cripto-análise Linear

cifra	complexidade na informação textos claros conhecidos	espaço complexidade	processamento complexidade
FEAL-4	5	30KB	6min
FEAL-6	100	100KB	40min
FEAL-8	2^{24}	280KB	10min

Cripto-análise Diferencial

A cripto-análise diferencial explora a alta probabilidade de ocorrência de relações entre diferenças entre textos claros e diferenças entre os correspondentes textos cifrados.

- É um **ataque texto claro escolhido**
  - O atacante é capaz de seleccionar textos claros e os correspondentes textos cifrados.
  - O atacante seleccionará pares de textos claros, X' e X'', que satisfaçam um dado ΔX, sabendo que para esse valor de ΔX, um dado valor de ΔY ocorre com uma probabilidade alta.

Cripto-análise Diferencial

Por exemplo, considere-se um sistema com entrada $X = [X_1 X_2 \dots X_n]$ e saída $Y = [Y_1 Y_2 \dots Y_n]$.
Sejam X' e X'' duas entradas no sistema com as correspondentes saídas Y' e Y''. A diferença nas entradas é dado por $\Delta X = X' \oplus X''$, consequentemente:

$$\Delta X = [\Delta X_1 \Delta X_2 \dots \Delta X_n], \qquad \text{com } \Delta X_i = X'_i \oplus X''_i.$$

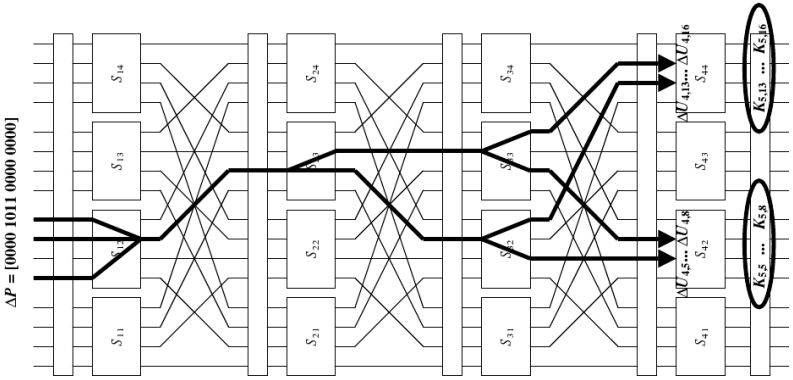
De forma semelhante, $\Delta Y = Y' \oplus Y''$ é a diferença na saída, e

$$\Delta Y = [\Delta Y_1 \Delta Y_2 \dots \Delta Y_n] \qquad \text{com } \Delta Y_i = Y'_i \oplus Y''_i.$$

Numa cifra aleatória, a probabilidade que uma dada diferença na saída, ΔY ocorra, dado uma diferença na entrada particular ΔX é de $1/2^n$ aonde n é o número de bits de X.

A cripto-análise diferencial tenta explorar o cenário no qual uma dada diferença ΔY ocorre, dado uma diferença na entrada ΔX particular, com uma alta probabilidade p_D (i.e., bastante maior do que $1/2^n$). O par $(\Delta X, \Delta Y)$ é referido como o diferencial.

Cripto-análise Diferencial



Resistência à Cripto-análise Diferencial

cifra	complexidade na informação textos claros escolhidos	espaço complexidade	processamento complexidade
FEAL-8	2^7 pares	—	2min
FEAL-16	2^{29} pares	—	2^{30} operações
FEAL-24	2^{45} pares	—	2^{46} operações
FEAL-32	2^{66} pares	—	2^{67} operações

Função Unidireccional

Definição (Função Unidireccional)

Uma função f de um conjunto X para um conjunto Y é dita uma função unidireccional ("one-way function") se $f(x)$ é "fácil de calcular" para todo o $x \in X$, mas "essencialmente para todos" os elementos $y \in \mathrm{Im}(f)$ é "computacionalmente difícil" achar um $x \in X$ tal que $f(x) = y$.

- Os termos "fácil de calcular" e "computacionalmente difícil" podem ser definidos de forma rigorosa.
- Com a utilização da frase "essencialmente para todos" pretende-se dizer que podem existir alguns elementos $y \in Y$ para os quais o cálculo de $x \in X$ tal que $y = f(x)$ é fácil, mas que no caso mais genérico tal não se verifica.