Standard de Chiffrement de Données : DES

DES : Data Encryption Standard
- 1973 : appel d'offre du National Bureau of Standards ;
- 1975 : publication du DES (modification de LUCIFER d'IBM) ;
- 1977 : adoption comme standard.
- révisé tous les 5 ans.
- fin probable : 1998

Algorithme du DES L'algorithme du DES prend en entrée un texte clair de 64 bits, une clé de 64 bits (dont les bits terminaux de chaques octets sont des bits de parité pour le contrôle des erreurs) et calcule un texte crypté sur 64 bits.

Algorithme général du DES

$DES(x : texte\ 64bits, K : clé\ 64bits) : 64bits$

$L_0R_0 = IP(x), (|L_0| = |R_0| = 32)$

Pour $i = 1$ à 16

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, T_i(K))$

finPour

résultat $IP^{-1}(R_{16}L_{16})$

$f(r : 32bits, k : 48bits) : 32bits$

$B = Exp(r) \oplus k = B_1 \ldots B_8, (|B_i| = 6)$

Pour $i = 1$ à 8

$B_i = b_1 \ldots b_6$

$C_i = S_i(b_1b_6, b_2b_3b_4b_5)$

finPour

résultat $P(C_1 \ldots C_8)$

Diversification de la clé

Principe : la clé subit une permutation, une série de rotations circulaires “par partie” puis une permutation inverse.

Algo. de diversification de la clé Les fonctions LS_j, $1 \leq j \leq 16$ sont des rotations circulaires vers la gauche d'un bit pour les indices 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14 et 15, et de deux bits pour les indices 1, 2, 9 et 16.

$T_i(k : 64 bits) : 48 bits$
  $k' = ote\_bits\_de\_parite(k)$
  $C_0 D_0 = PC\text{–}1(k'), (|C_0|{=}|D_0|{=}\ 28)$
  Pour $j = 1$ à i
    $C_j = LS_j(C_{j-1})$
    $D_j = LS_j(D_{j-1})$
  finPour
  résultat $PC\text{–}2(C_i, D_i)$

rem.: Les fonctions de permutation $T_i(K), 1 \leq i \leq 16$ sont calculables à l'avance.

Modes d'utilisation du DES

ECB (electronic codebook mode) :
mode courant ;

IV : une valeur initiale arbitraire.

CBC (cipher block chaining mode) :

$CBC(x_1, x_2, \ldots : 64bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$y_i = DES(y_{i-1} \oplus x_i)$
finTantque

$CBC^{-1}(y_1, y_2, \ldots : 64bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$x_i = y_{i-1} \oplus DES^{-1}(y_i)$
finTantque

Modes d'utilisation du DES (suite)

OFB (output feedback mode) :
Chiffrement en chaîne synchrone

$OFB = (x_1, x_2, \ldots : 64 bits)$
bloc initial $z_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$z_i = DES(z_{i-1})$
$y_i = z_i \oplus x_i$
finTantque

$OFB^{-1}(y_1, y_2, \ldots : 64 bits)$
bloc initial $z_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$z_i = DES(z_{i-1})$
$x_i = z_i \oplus y_i$
finTantque

Modes d'utilisation du DES (suite)

CFB (cipher feedback mode) :

$CFB = (x_1, x_2, \ldots : 64 bits)$
initial bloc $y_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$z_i = DES(y_{i-1})$
$y_i = z_i \oplus x_i$
finTantque

$CFB^{-1}(y_1, y_2, \ldots : 64 bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$z_i = DES(y_{i-1})$
$x_i = z_i \oplus y_i$
finTantque