Ataque Meet in the Middle

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://cryptomex.org
@cryptomex

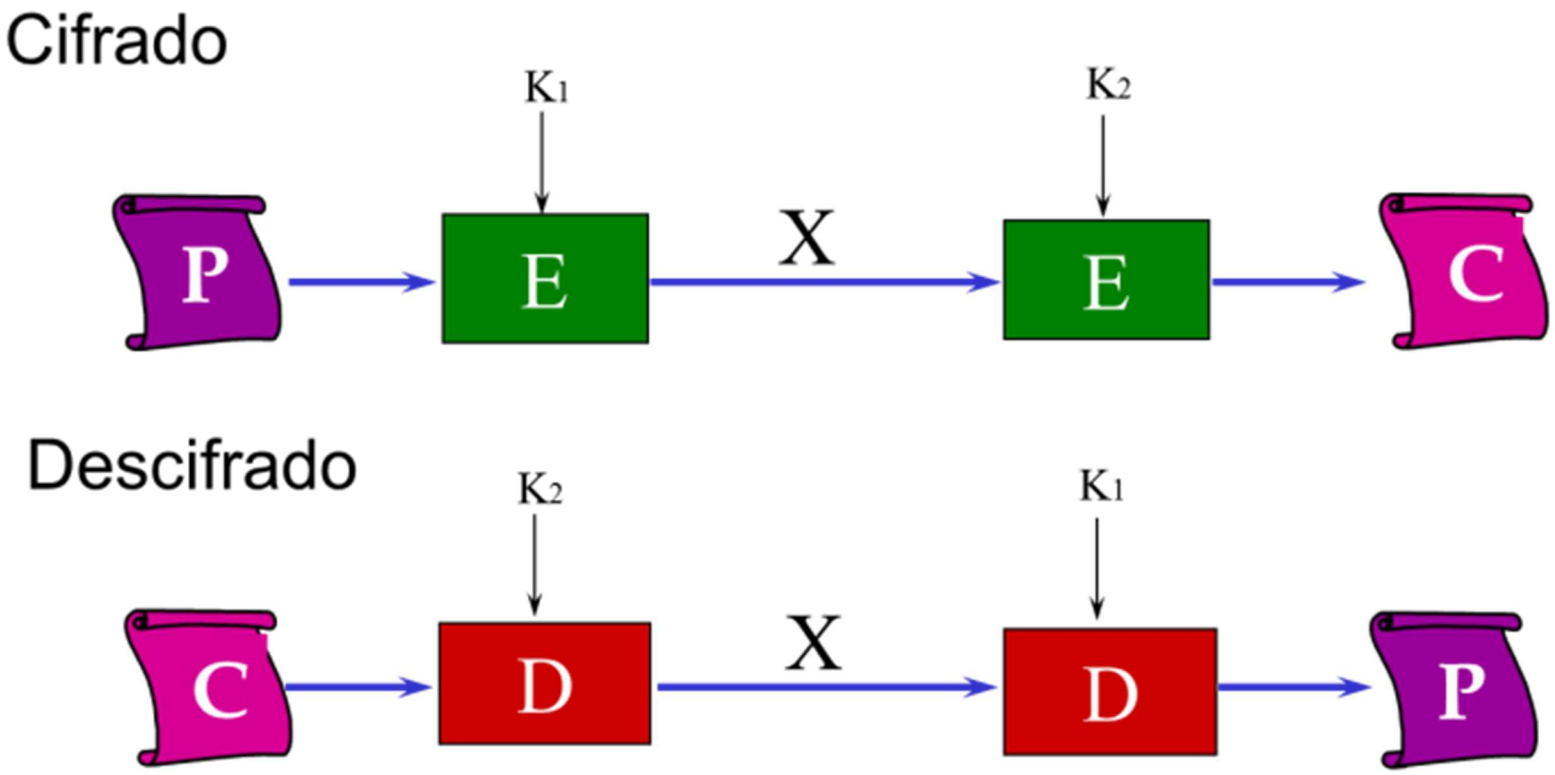
Objetivo ataque criptográfico

- Recuperar la llave de cifrado
- Descifrar el criptograma
- En 2 DES
  - Recuperar la(s) llave(s) de cifrado

Doble DES

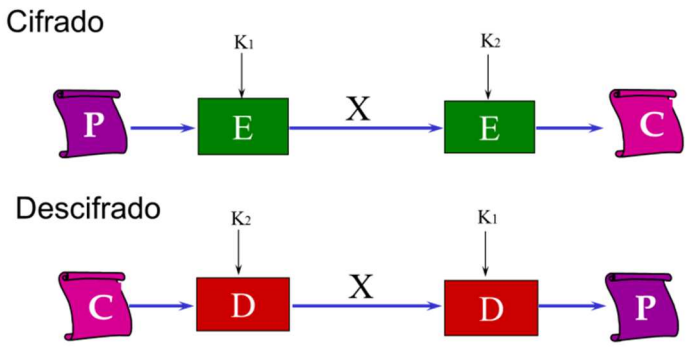
- Uso de dos llaves
- Cifrado
- Descifrado
- Longitud de cada llave: 56
- Work factor: 56 x 2 = 112

2 DES



Ataque Meet in the Middle

- $C = E_{K2}(E_{K1}(P))$
- Entonces: $X = E_{K1}(P) = D_{K2}(C)$
- Dado un par conocido (P, C)
  - Cifrar P con todas las 2^{56} llaves posibles de K1
  - Descifrar C con todas las 2^{56} llaves posibles de K2
  - Buscar X, tal que $X = E_{K1}(P) = D_{K2}(C)$
  - Llaves: K1 y k2



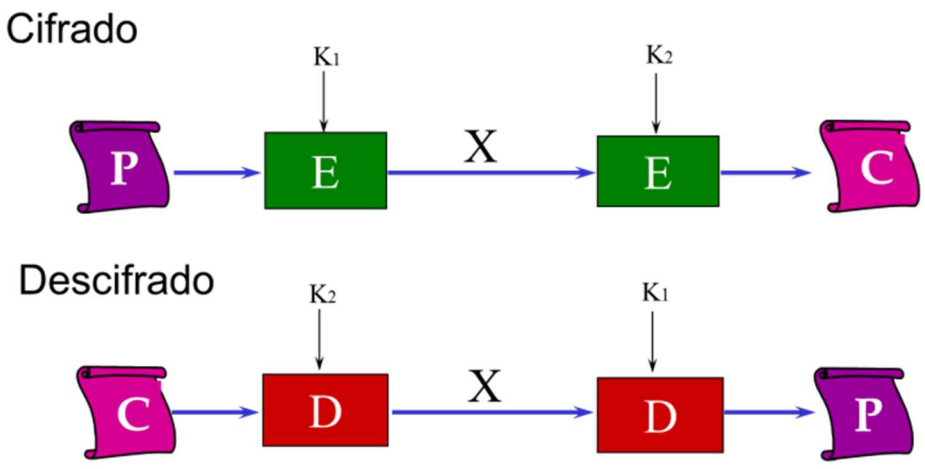
Otro enfoque

- $C = E_{K2}(E_{K1}(P))$
- Dado un mar (C, P), se tiene $E_{K1}(P) = D_{K2}(C)$
- Construir tabla con el resultado de cifrar C con las 2^{56} combinaciones de K_1
- Buscar, por cada valor posible de K_2, si $D_{K2}(C)$ esta en la tabla
- Se tendrán que probar un máximo de 2^{56} opciones
- Wor k factor: $2^{56} + 2^{56}$, y no 2^{112}

Esquema general

K_1^i	Valor Llave	Resultado $Ek_1^i(P)$
K_1^1	0000 … 0000	C_1
K_1^2	0000 … 0001	C_2
K_1^3	0000 … 0010	C_3
K_1^4	0000 … 0011	C_4
K_1^5	0000 … 0100	C_5
K_1^5	0000 … 0101	C_6
K_1^6	0000 … 0110	C_7
K_1^7	0000 … 0111	C_8
	:	
	:	
	:	
$K_1^{((2^56)-7)}$	0000 … 1000	$C_{((2^56)-7)}$
$K_1^{((2^56)-6)}$	0000 … 1001	$C_{((2^56)-6)}$
$K_1^{((2^56)-5)}$	0000 … 1010	$C_{((2^56)-5)}$
$K_1^{((2^56)-4)}$	0000 … 1011	$C_{((2^56)-4)}$
$K_1^{((2^56)-3)}$	0000 … 1100	$C_{((2^56)-3)}$
$K_1^{((2^56)-2)}$	0000 … 1101	$C_{((2^56)-2)}$
$K_1^{((2^56)-1)}$	0000 … 1110	$C_{((2^56)-1)}$
$K_1^{((2^56))}$	0000 … 1111	$C_{((2^56))}$

$$Dk_2^i(P) = X_i$$



Ejemplo

- Tamaño Texto Plano: 3 bits
- Tamaño Llave: 2 bits

Llave	Valor
K_1	00
K_2	01
K_3	10
K_4	11

i	P_i	$E_{K1}(P_i)$	$E_{K2}(P_i)$	$E_{K3}(P_i)$	$E_{K4}(P_i)$
1	000	010	110	111	011
2	001	100	000	010	001
3	010	110	111	000	010
4	011	111	010	100	000
5	100	101	011	001	111
6	101	000	001	101	110
7	110	011	101	110	101
8	111	001	100	011	100

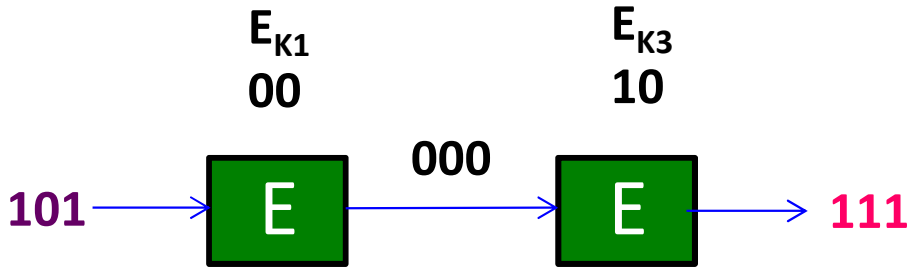
Aplicando el ataque

- Considerar el siguiente texto plano con llaves K_1 y K_3
  - P = 101

    $E_{K1}(101) = 000$

    $E_{K3}(000) = 111$
  - D = 111

i	P_i	$E_{K1}(P_i)$	$E_{K2}(P_i)$	$E_{K3}(P_i)$	$E_{K4}(P_i)$
1	000	010	110	111	011
2	001	100	000	010	001
3	010	110	111	000	010
4	011	111	010	100	000
5	100	101	011	001	111
6	101	000	001	101	110
7	110	011	101	110	101
8	111	001	100	011	100



$E_{K1}(101) = 000$

$E_{K2}(101) = 001$

$E_{K3}(101) = 101$

$E_{K4}(101) = 110$

$D_{K1}(111) = 011$

$D_{K2}(111) = 010$

$D_{K3}(111) = 000$