Block ciphers

Exhaustive Search Attacks

Exhaustive Search for block cipher key

Goal: given a few input output pairs $(m_i, c_i = E(k, m_i))$ i=1,..,3
find key k.

Lemma: Suppose DES is an ***ideal cipher***

(2^{56} random invertible functions $\pi_1, \ldots, \pi_{2^{56}} : \{0,1\}^{64} \to \{0,1\}^{64}$)

Then $\forall$ m, c there is at most **one** key k s.t. c = DES(k, m)

Proof: with prob. $\geq 1 - 1/256 \approx 99.5\%$

$$Pr[\exists k' \neq k : c = DES(k,m) = DES(k',m)] \leq$$

$$\leq \sum_{k' \in \{0,1\}^{56}} Pr[DES(k,m) = DES(k',m)] \leq 2^{56} \cdot \frac{1}{2^{64}} = \frac{1}{2^8}$$

Exhaustive Search for block cipher key

For two DES pairs $(m_1, c_1=DES(k, m_1))$, $(m_2, c_2=DES(k, m_2))$

unicity prob. $\approx 1 - 1/2^{71}$

For AES-128: given two inp/out pairs, unicity prob. $\approx 1 - 1/2^{128}$

$\Rightarrow$ two input/output pairs are enough for exhaustive key search.

DES challenge

msg = "The unknown messages is: XXXX … "

CT = c_1 c_2 c_3 c_4

Goal: find $k \in \{0,1\}^{56}$ s.t. $DES(k, m_i) = c_i$ for i=1,2,3

1997: Internet search -- **3 months**

1998: EFF machine (deep crack) -- **3 days** (250K $)

1999: combined search -- **22 hours**

2006: COPACOBANA (120 FPGAs) **-- 7 days** (10K $)

⇒ 56-bit ciphers should not be used !! (128-bit key ⇒ 2^{72} days)

Strengthening DES against ex. search

Method 1: **Triple-DES**

- Let $E : K \times M \longrightarrow M$ be a block cipher
- Define **3E**: $K^3 \times M \longrightarrow M$ as

$$\mathbf{3E}\big((k_1,k_2,k_3), m\big) = E(k_1, D(k_2, E(k_3, m)))$$

$k_1 = k_2 = k_3 \Rightarrow$ single DES

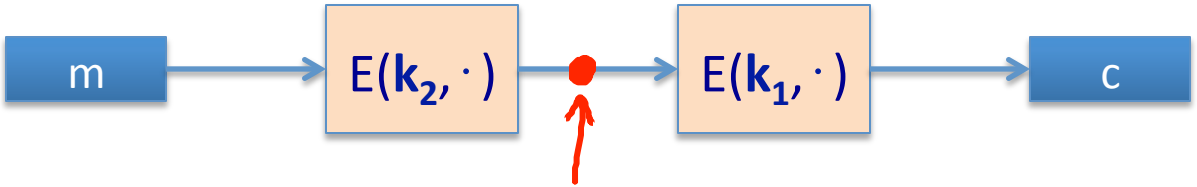
For 3DES: key-size = 3×56 = 168 bits. 3×slower than DES.

(simple attack in time $\approx 2^{118}$)

Why not double DES?

- Define $2E\big((k_1,k_2), m\big) = E\big(k_1, E(k_2, m)\big)$

key-len = 112 bits for DES



Find (k_1, k_2) s.t.
$E(k_1, E(k_2, M)) = C$
Equivalently:
$E(k_2, M) = D(k_1, C)$

Attack: $M = (m_1,\ldots, m_{10})$, $C = (c_1,\ldots,c_{10})$.

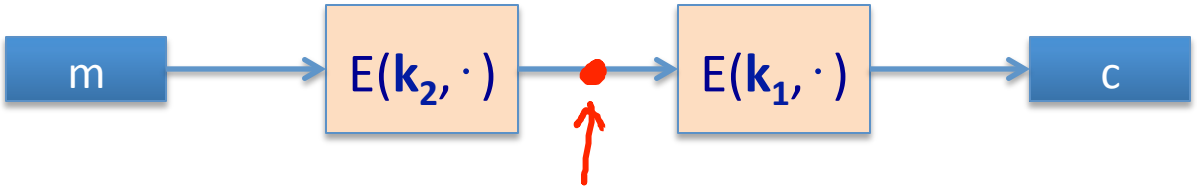
- step 1: build table.

  sort on 2nd column

$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

2^{56} entries

Meet in the middle attack



$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

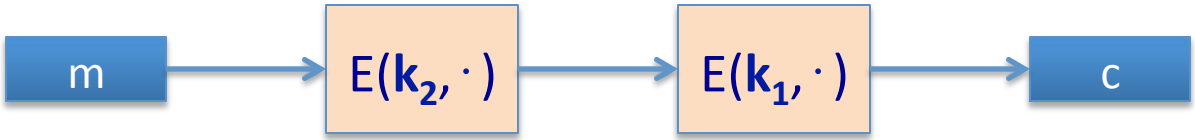
Attack: $M = (m_1,\ldots, m_{10})$, $C = (c_1,\ldots,c_{10})$

- step 1: build table.
- Step 2: for all $k \in \{0,1\}^{56}$ do:

  test if $D(k, C)$ is in 2nd column.

if so then $E(k^i,M) = D(k,C) \Rightarrow (k^i,k) = (k_2,k_1)$

Meet in the middle attack

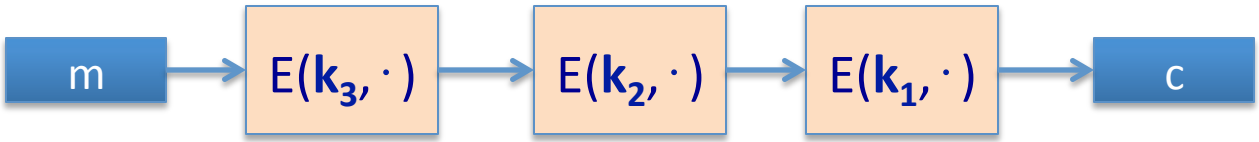


Time = $2^{56}\log(2^{56})$ + $2^{56}\log(2^{56})$ $< 2^{63}$ $<<$ 2^{112} , space $\approx 2^{56}$

build + sort table

search in table

Same attack on 3DES: Time = 2^{118} , space $\approx 2^{56}$



Method 2: DESX

$E : K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ a block cipher

Define EX as $EX((k_1,k_2,k_3), m) = k_1 \oplus E(k_2, m \oplus k_3)$

For DESX: key-len = 64+56+64 = 184 bits

… but easy attack in time $2^{64+56} = 2^{120}$ (homework)

Note: $k_1 \oplus E(k_2, m)$ and $E(k_2, m \oplus k_1)$ does nothing !!

End of Segment