西安电子科技大学
XIDIAN UNIVERSITY

Exhaustive Search Attacks

西安电子科技大学
XIDIAN UNIVERSITY

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

with prob. ≥ 1 – 1/256 ≈ 99.5%

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

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

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

unicity prob. ≈ $1 - 1/2^{71}$

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

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 $)

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

西安电子科技大学 XIDIAN UNIVERSITY

- 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 $\approx 2^{118}$)

$$m \rightarrow E(k_2,\cdot) \rightarrow E(k_1,\cdot) \rightarrow c$$

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

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

$$\text{Time} = \underbrace{2^{56}\log(2^{56})}_{\text{build + sort table}} + \underbrace{2^{56}\log(2^{56})}_{\text{search in table}} < 2^{63} \ll 2^{112} \ , \quad \text{space} \approx 2^{56}$$

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

$$m \rightarrow E(k_3, \cdot) \rightarrow E(k_2, \cdot) \rightarrow E(k_1, \cdot) \rightarrow c$$

西安电子科技大学 XIDIAN UNIVERSITY

Method 2: DESX

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

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

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

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

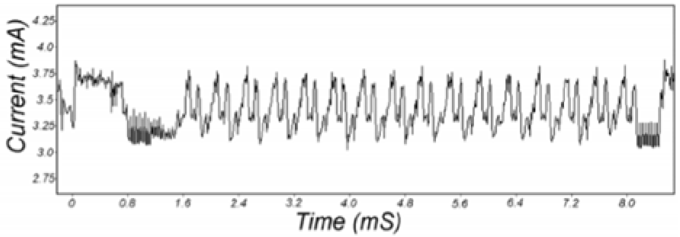
Note: $k_1 \oplus E(k_2, m)$ and $E(k_2, m \oplus k_1)$ does nothing !!

More attacks on block ciphers

Attacks on the implementation

1. Side channel attacks:
   – Measure **time** to do enc/dec,   measure **power** for enc/dec

smartcard



[Kocher, Jaffe, Jun, 1998]

2. Fault attacks:
   – Computing errors in the last round expose the secret key k

⇒ do not even implement crypto primitives yourself …

西安電子科技大學 XIDIAN UNIVERSITY

Linear attacks

$$\Pr\Big[\underbrace{m[i_1]\oplus\cdots\oplus m[i_r]}_{\text{subset of msg bits}} \oplus \underbrace{c[j_j]\oplus\cdots\oplus c[j_v]}_{\text{subset of ciphertext bits}} = \underbrace{k[l_1]\oplus\cdots\oplus k[l_u]}_{\text{subset of key bits}}\Big] = \tfrac{1}{2} + \varepsilon$$

For some ε. For DES, this exists with $\varepsilon = 1/2^{21} \approx 0.0000000477$

Thm: given $1/\varepsilon^2$ random $\big(m,\ c=\mathrm{DES}(k, m)\big)$ pairs then

$$k[l_1,\ldots,l_u] = \mathrm{MAJ}\left[\ m[i_1,\ldots,i_r] \oplus c[j_j,\ldots,j_v]\ \right]$$

with prob. $\geq 97.7\%$

$\Rightarrow$ with $1/\varepsilon^2$ inp/out pairs can find $k[l_1,\ldots,l_u]$ in time $\approx 1/\varepsilon^2$.

For DES, $\varepsilon = 1/2^{21}$ $\Rightarrow$

with 2^{42} inp/out pairs can find $k[l_1,\dots,l_u]$ in time 2^{42}

Roughly speaking: can find 14 key “bits” this way in time 2^{42}

Brute force remaining $56-14=42$ bits in time 2^{42}

Total attack time $\approx 2^{43}$ ($\ll 2^{56}$) with 2^{42} random inp/out pairs

西安电子科技大学 XIDIAN UNIVERSITY

Quantum attacks

Generic search problem:

Let $f: X \longrightarrow \{0,1\}$ be a function.

Goal: find $x \in X$ s.t. $f(x)=1$.

Given m, $c=E(k,m)$ define

$$f(k) = \begin{cases} 1 & \text{if } E(k,m) = c \\ 0 & \text{otherwise} \end{cases}$$

Grover $\Rightarrow$ quantum computer can find k in time $O(|K|^{1/2})$

DES: time $\approx 2^{28}$, AES-128: time $\approx 2^{64}$

quantum computer $\Rightarrow$ 256-bits key ciphers (e.g. AES-256)

西安电子科技大学
XIDIAN UNIVERSITY

End of Segment