

Differential Cryptanalysis

Linear Cryptanalysis

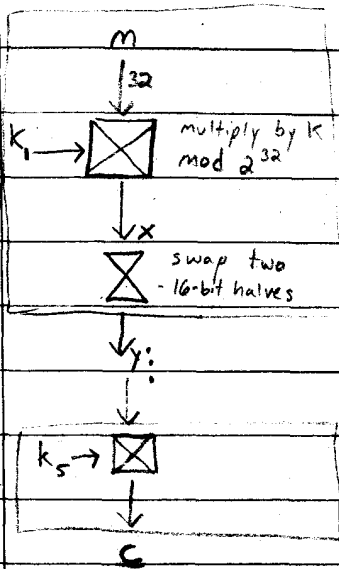
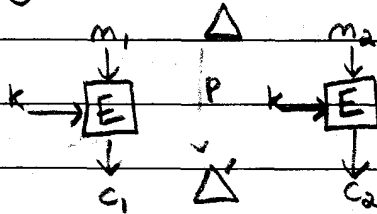
10/02

Steps to Attack

- ① Build a chosen plaintext distinguisher
- ② Convert to key recovery attack - chosen plaintext
- ③ Convert to known plaintext

Differential Cryptanalysis

Strategy: find differences preserved by cipher



k 's must be odd
155-bit key

consider

$$m \quad m' = 2m$$

$$x \quad x' = 2x$$

$$y = [x_{15} \ x_{14} \ \dots \ x_0 \mid x_{31} \ \dots \ x_{16}]$$

$$y' = [x_{15} \ \dots \ x_0 \ 0 \mid x_{30} \ \dots \ x_{16}]$$

$$x_{15} \text{ must} = 0$$

$$x_{31} \text{ must} = 0$$

$$y' = 2y \text{ iff } x_{15} = x_{31} = 0 \quad P_r \approx \frac{1}{4}$$

after 4 rounds, $P_r \approx (\frac{1}{4})^4$

$(m, 2m) \xrightarrow{E} (c, 2c)$ chosen plaintext distinguisher:

- ① Query oracle on 2^8 message pairs $(m, 2m)$
- ② If any output pair is $(c, 2c)$ return 1 else return 0

Key recovery

If (m, m') is a right pair, then we know
 $X = k'm$ has $X_{15} = X_{31} = 0$

① Query cipher on 2^{12} pairs to obtain 2^4 right pairs
 $(m_1, m'_1), \dots, (m_{15}, m'_{15})$

② For each possible k'

Let $X^1, X^2, \dots, X^{16} = k'm_1, \dots, k'm_{16}$

If $X^i_{15} = X^i_{31} = 0 \quad \forall i = 1, \dots, 16$

output k'

Note: will likely output 1 k'

Work = 2^{35}

③ Compute y^1, \dots, y^{16} and repeat from step ②

Work = 2^{37}

Chosen \rightarrow known plaintext

① collect 2^{23} messages

② we will have 2^{45} pairs

③ $\frac{2^{45}}{2^{32}} = 2^{13}$ pairs will be of the form $(m, 2m)$

Use previous attack

"right" pair $\rightarrow (m, 2m) \xrightarrow{E} (c, 2c)$

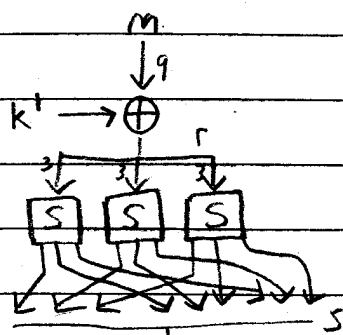
Linear Cryptanalysis "linear differential cryptanalysis tutorial"

Strategy - find linear relations among inputs, key outputs

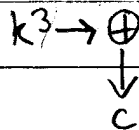
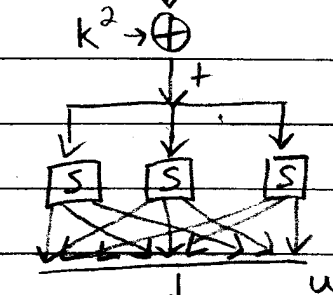
e.g. $c_{12} \oplus c_{13} = m_1 \oplus k_7$

$c_{12} \oplus c_{13} \oplus m_1 = k_7$

bias = how far is P from $\frac{1}{2}$



	input			output		
S:	a	b	c	x	y	z
	0	0	0	0	1	0
	0	0	1	1	1	0
	0	1	0	0	0	0
	0	1	1	1	1	1
	1	0	0	0	0	1
	1	0	1	1	0	1
	1	1	0	1	0	0
	1	1	1	0	1	1



$x = a \oplus c$ with $P_r \frac{3}{4}$
 $y = a \oplus 1$ with $P_r \frac{3}{4}$
 $z = a$ with $P_r \frac{3}{4}$

$r_i = m_i \oplus k_i^1$

$r_i \oplus m_i \oplus k_i^1 = 0$ ($P_r = 1$)

$s_0 \oplus r_0 \oplus r_2 = 0$ ($P_r = \frac{3}{4}$)

$t_0 \oplus s_0 \oplus k_0^2 = 0$ ($P_r = 1$)

$u_0 \oplus t_0 = 0$ ($P_r = \frac{3}{4}$)

$c_0 \oplus u_0 \oplus k_0^3 = 0$ ($P_r = 1$)

$m_0 \oplus k_0^1 \oplus m_2 \oplus k_2^1$

$\oplus k_0^2 \oplus k_0^3 \oplus c_0 = 0$

with $P_r = \frac{3}{4} \cdot \frac{3}{4} + \frac{1}{16} = \frac{5}{8}$