# Cryptanalysis

## Goal

- Key Recovery
- Message Recovery
- Distinguishing

## Power

- Ciphertext only Attack (CA)
- Known Plaintext Attack (KPA)
- Chosen Plaintext Attack (CPA) [Oracle Access to Encryption]
- Chosen Ciphertext Attack (CCA) [Oracle Access to Encryption, Decryption]

## Kirkchoff's Principle

Except key, everything is known to the adversary

# Complexity

- Data / Query : # queries to the oracle
- Time : total time required to mount the attack (Time Unit ⇒ C/T from the P/T & key (B/C computation))
- Memory : total Storage required

Complexity = (D, T, M)

# Complexity

- Data / Query : # queries to the oracle (includes (P/T-C/T) pairs)
- Time : total time required to mount the attack (Time Unit ⇒ C/T from the P/T & Key (B/C computation))
- Memory : total storage required

Complexity = (D, T, M)

# Brute-Force Attacks

(Applicable to any B/Cs)

$E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

$k \geq n$

## (1) Key Recovery Attack (KPA)

- Suppose you have a plaintext-ciphertext pair. $(M_1, C_1)$
- For all keys $k \in \{0,1\}^k$, Check if $E_k(m_1) \stackrel{?}{=} C_1$

  If unique return that key

  else repeat

### Complexity

Data → $k/n$

Time → $2^k$

Memory → negl

($M,C$) pairs + valid-keys)

$\left(\frac{k}{n}, 2^k, \text{negl}\right)$

⇓

k should be large

## (2) Message Recovery Attack

- Make Oracle queries for all messages

$$(P_1, C_1), \ldots\ldots, (P_{2^n}, C_{2^n})$$

- Store all the values
- Return the P/T corresponding to the ciphertext

### Complexity

$D = 2^n$

$T = n e g e$

$M = 2n \cdot 2^n$ (bit)

$T \approx D^2$

$\begin{cases} D \approx 2^{64} \\ T \approx 2^{128} \end{cases}$ (NIST recommended)

# Short-cut Attacks

Attacks better than Brute Force Attack
(Complexity)

- Differential Cryptanalysis (CPA) *
- Linear Cryptanalysis (CPA) *
- Impossible Differential Cryptanalysis (CPA) *
- Integral Cryptanalysis (CPA) *
- Boomerang Attacks (CCA)
- Related key Attacks

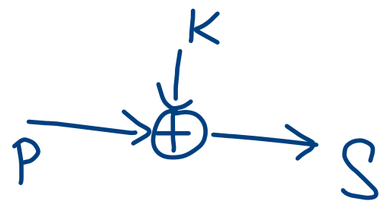
└ $(k/n,\ 2^k,\ negl)$
└ $(2^n,\ negl,\ 2n.2^n)$

$k=128,\ n=64$

$(*,\ 2^{126},\ *) \Rightarrow$ Valid Shortcut attack
$(2^{62},\ *,\ *) \Rightarrow$

# Differential Cryptanalysis

## Motivation




- Adversary has no information about S. (K is unknown)
- If you encrypt two P/Ts $P_1$, $P_2$ then

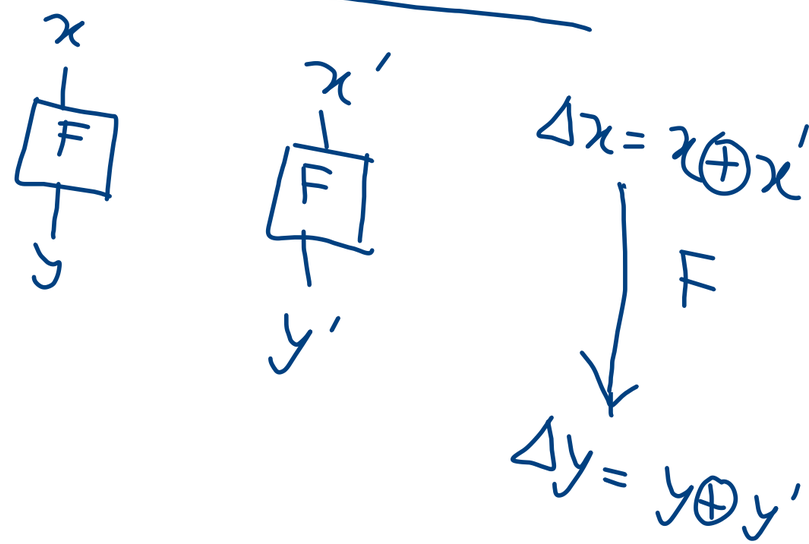
$$S_1 \oplus S_2 = P_1 \oplus P_2$$

(Difference of the state is known, which is indep of the key)

⇓

(Exploits the differential property.)

## Difference Propagation



# Toy Example

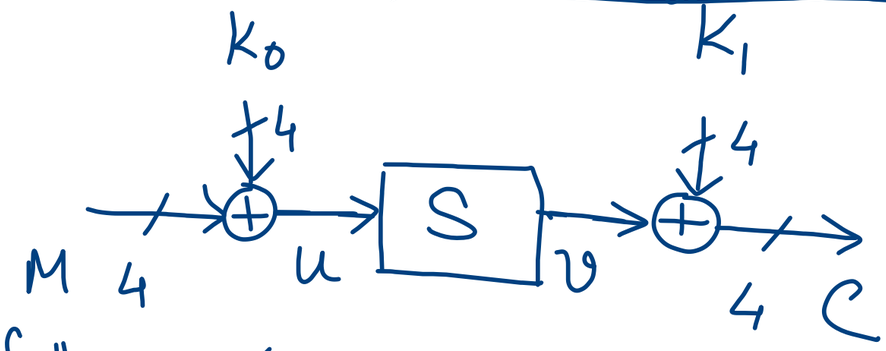
$9 \oplus 7 = 1001 \oplus 0111 = 1110 \to \in$

$6 \oplus 7 = 0110 \oplus 0111 = 0001 \to 1$

$A \to 1010$, $5 \to 0101$, $F \to 1111$

$0111 \oplus 1000 = 1111$

## Key-Recovery




$$\begin{cases} M, C \in \{0,1\}^4 \\ K = (K_0, K_1) \in \{0,1\}^8 \end{cases}$$

Suppose, I have the following (P/T, C/T) pairs - (A, 9), (5, 6)

- Set $m_0 = A$, $m_1 = 5$.
- $u_0 \oplus u_1 = m_0 \oplus m_1 = F$
- Guess $K_1$, compute $v_0, v_1$.
- Check if $S^{-1}(v_0) \oplus S^{-1}(v_1) \stackrel{?}{=} F$
- If yes, then $K_1$ is a possible valid choice.
- Find $K_1$
- Find $K_0$ from $K_1$ & any (P/T, C/T) pair.

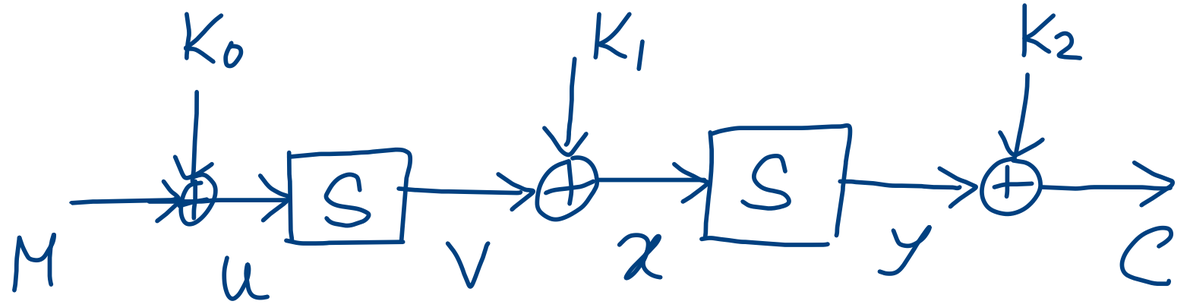
All possible Values of $K_1$

**Complexity** $(2, 2^4, *)$

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S(x) | 6 | 4 | C | 5 | 0 | 7 | 2 | E | 1 | F | 3 | D |

| x | C | D | E | F |
|---|---|---|---|---|
| $S^{-1}(x)$ | 8 | A | 9 | B |

$S^{-1}(E) \oplus S^{-1}(1) = 7 \oplus 8 = F$




$(*, 2^8, *)$

(F)

- $(u_0 \oplus u_1) = (m_0 \oplus m_1) \rightarrow$ Known
- Guess $K_2$, Compute $y_0, y_1$
- Compute $x_0, x_1$
- $v_0 \oplus v_1 = x_0 \oplus x_1 \rightarrow$ known
- $v_0 \oplus v_1 \stackrel{?}{=} D$

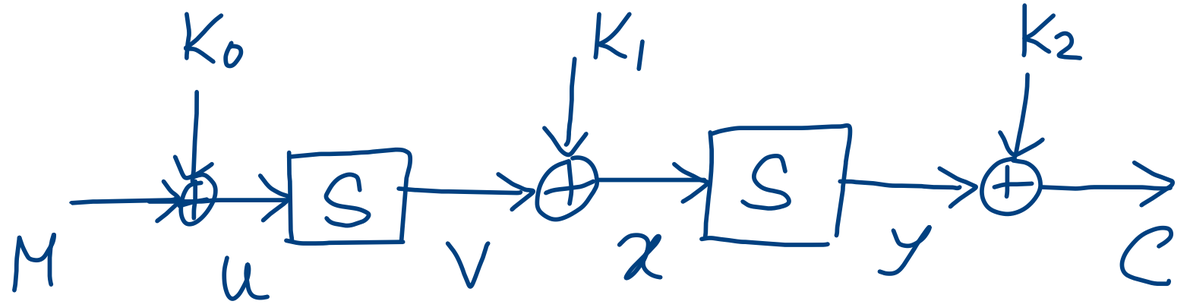
- Repeat }

$$\Delta u \xrightarrow[S]{} \Delta v$$

$$Pr\left[\text{I/P Diff } F \xrightarrow[S]{} \text{O/P Diff } D\right] = \frac{10}{16}$$

High

- Choose $m_0, m_1$ s.t. $m_0 \oplus m_1 = F$ (CPA)




$(*, 2^8, *)$

(F)

- $(u_0 \oplus u_1) = (m_0 \oplus m_1) \rightarrow$ Known
- Guess $K_2$, Compute $y_0, y_1$
- Compute $x_0, x_1$
- $v_0 \oplus v_1 = x_0 \oplus x_1 \rightarrow$ known
- $v_0 \oplus v_1 \stackrel{?}{=} D$

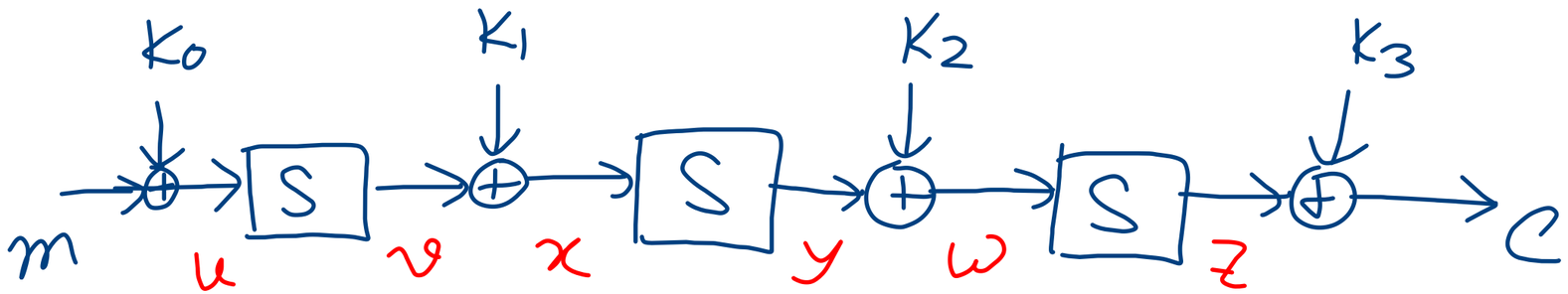
- Repeat }

$$\Delta u \xrightarrow[S]{} \Delta v$$

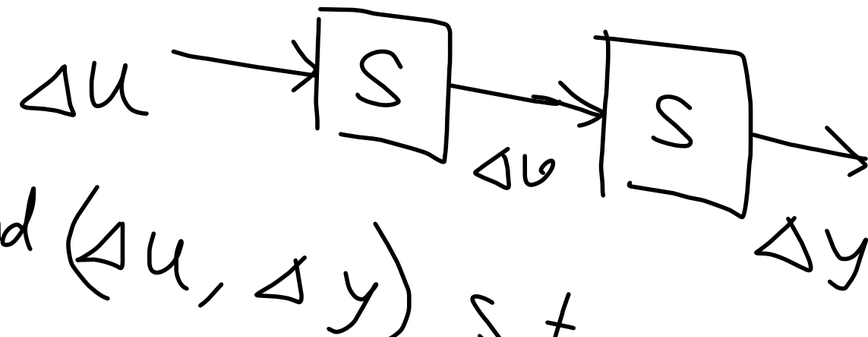
$$Pr\left[\text{I/P Diff } F \xrightarrow[S]{} \text{O/P Diff } D\right] = \frac{10}{16}$$

- Choose $m_0, m_1$ s.t. $m_0 \oplus m_1 = F$ (CPA)

↓ High




- $\Delta u$ known
- Guess $K_3$, $z_0, z_1$ known, $w_0, w_1$ known
- $\Delta y = y_0 \oplus y_1$ known




Find $(\Delta u, \Delta y)$ s.t.

$Pr[\Delta u \xrightarrow{S,S} \Delta y] \rightarrow$ high