# Chosen Plaintext Attack and Pseudorandom Function

Yu Zhang

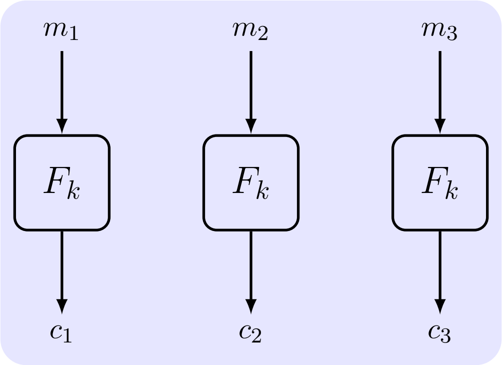
Harbin Institute of Technology

Cryptography, Autumn, 2018

# Outline

# Content

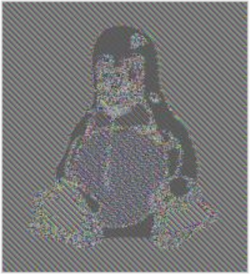
# Electronic Code Book (ECB) Mode



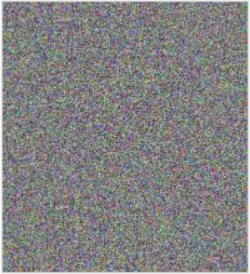

- Q: is it indistinguishable in the presence of an eavesdropper?

# Attack on ECB mode

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

# Chosen-Plaintext Attacks (CPA)

**CPA**: the adversary has the ability to obtain the encryption of plaintexts of its choice

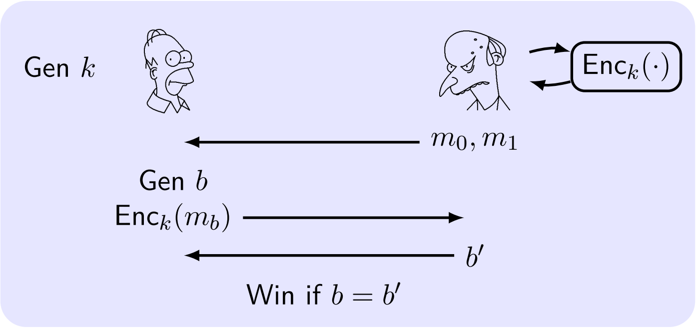
**A story in WWII**

- Navy cryptanalysts believe the ciphertext "AF" means "Midway island" in Japanese messages
- But the general did not believe that Midway island would be attacked
- Navy cryptanalysts sent a plaintext that the freshwater supplies at Midway island were low
- Japanese intercepted the plaintext and sent a ciphertext that "AF" was low in water
- The US forces dispatched three aircraft carriers and won

# Security Against CPA

The CPA indistinguishability experiment $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$:

1. $k \leftarrow \mathsf{Gen}(1^n)$
2. $\mathcal{A}$ is given input $1^n$ and **oracle access** $\mathcal{A}^{\mathsf{Enc}_k(\cdot)}$ to $\mathsf{Enc}_k(\cdot)$, outputs $m_0, m_1$ of the same length
3. $b \leftarrow \{0,1\}$. Then $c \leftarrow \mathsf{Enc}_k(m_b)$ is given to $\mathcal{A}$
4. $\mathcal{A}$ **continues to have oracle access** to $\mathsf{Enc}_k(\cdot)$, outputs $b'$
5. If $b' = b$, $\mathcal{A}$ succeeded $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi} = 1$, otherwise 0



# CPA Security

**Definition 1**

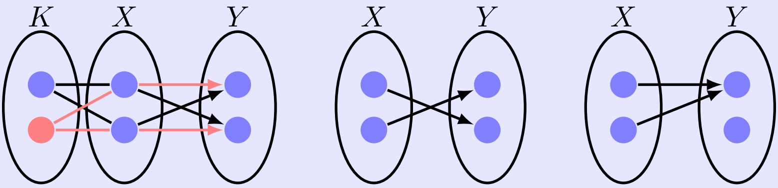
$\Pi$ has **indistinguishable encryptions under a CPA (CPA-secure)** if $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

- Q: Is any cipher we have learned so far CPA-secure? Why?

# Content

# Concepts on Pseudorandom Functions




- **Keyed function** $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$
  $F_k : \{0,1\}^* \to \{0,1\}^*$, $F_k(x) \stackrel{\text{def}}{=} F(k,x)$
- **Look-up table** $f$: $\{0,1\}^n \to \{0,1\}^n$ with size $=$ ? bits
- **Function family** $\mathsf{Func}_n$: all functions $\{0,1\}^n \to \{0,1\}^n$.
  $|\mathsf{Func}_n| = 2^{n \cdot 2^n}$
- **Length Preserving**: $\ell_{key}(n) = \ell_{in}(n) = \ell_{out}(n)$

# Definition of Pseudorandom Function

**Intuition**: A PRF $F$ generates a function $F_k$ that is indistinguishable from truly random selected function $f$ (look-up table) in $\mathsf{Func}_n$.
However, the function has **exponential length**. Give $D$ the deterministic **oracle access** $D^{\mathcal{O}}$ to the functions $\mathcal{O}$.

**Definition 2**

An efficient length-preserving, keyed function $F$ is a **pseudorandom function (PRF)** if $\forall$ PPT distinguishers $D$,

$$\left|\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1]\right| \le \mathsf{negl}(n),$$

where $f$ is chosen *u.a.r* from $\mathsf{Func}_n$.

**Q: Is the fixed-length OTP a PRF?**

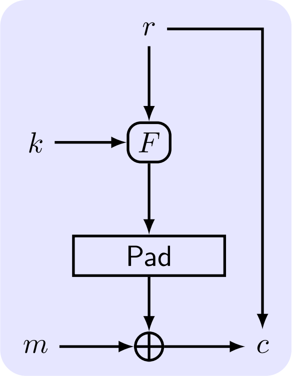
# Questions

**Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF. Is $G$ a secure PRF?**

- $G((k_1, k_2), x) = F(k_1, x) \| F(k_2, x)$
- $G(k, x) = \begin{cases} F(k, x) & \text{when } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$
- $G(k, x) = F(k, x) \bigoplus F(k, x \oplus 1^n)$

# Content

# CPA-Security from Pseudorandom Function




### Construction 3

- *Fresh random string $r$.*
- $F_k(r)$*:* $|k| = |m| = |r| = n$.
- Gen*:* $k \in \{0,1\}^n$.
- Enc*:* $s := F_k(r) \oplus m$,
  $c := \langle r, s \rangle$.
- Dec*:* $m := F_k(r) \oplus s$.

### Theorem 4

*If $F$ is a PRF, this fixed-length encryption scheme $\Pi$ is CPA-secure.*

# Proof of CPA-Security from PRF

**Idea**: First, analyze the security in an idealized world where $f$ is used in $\tilde{\Pi}$; next, claim that if $\Pi$ is insecure when $F_k$ was used then this would imply $F_k$ is not PRF by reduction.

**Proof.**

(1) Analyze $\Pr[\text{Break}]$, Break means $\text{PrivK}^{\text{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1$:
$\mathcal{A}$ collects $\{\langle r_i, f(r_i)\rangle\}$, $i = 1, \ldots, q(n)$ with $q(n)$ queries;
The challenge $c = \langle r_c, f(r_c) \oplus m_b \rangle$.

- Repeat: $r_c \in \{r_i\}$ with probability $\frac{q(n)}{2^n}$. $\mathcal{A}$ can know $m_b$.
- $\overline{\text{Repeat}}$: As OTP, $\Pr[\text{Break}] = \frac{1}{2}$

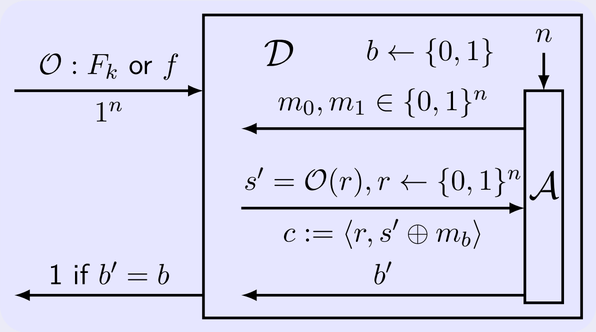
$$\begin{aligned}\Pr[\text{Break}] &= \Pr[\text{Break} \wedge \text{Repeat}] + \Pr[\text{Break} \wedge \overline{\text{Repeat}}] \\ &\leq \Pr[\text{Repeat}] + \Pr[\text{Break}|\overline{\text{Repeat}}] \\ &\leq \frac{q(n)}{2^n} + \frac{1}{2}.\end{aligned}$$

□

# Proof of CPA-Security from PRF (Cont.)

**Proof.**

(2) Reduce $D$ to $\mathcal{A}$:

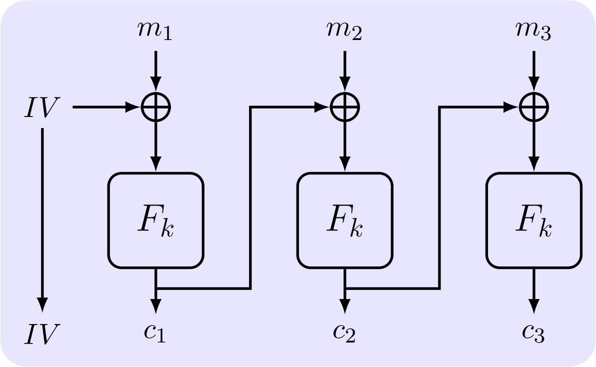



$\Pr[D^{F_k(\cdot)}(1^n) = 1] = \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} + \varepsilon(n)$.

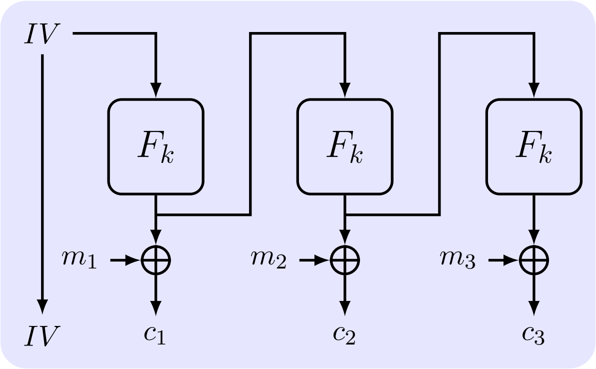
$\Pr[D^{f(\cdot)}(1^n) = 1] = \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1] = \Pr[\mathsf{Break}] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.

$\Pr[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \geq \varepsilon(n) - \frac{q(n)}{2^n}$. $\varepsilon(n)$ is negligible. $\square$

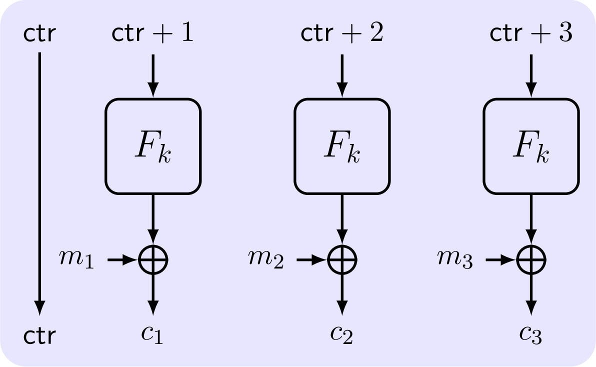
# Cipher Block Chaining (CBC) Mode



# Output Feedback (OFB) Mode



# Counter (CTR) Mode




- $ctr$ is an $IV$

# $IV$ Should Not Be Predictable

If $IV$ is predictable, then CBC/OFB/CTR mode is not CPA-secure.
Q: Why? (homework)

**Bug in SSL/TLS 1.0**

$IV$ for record $\#i$ is last CT block of record $\#(i-1)$.

**API in OpenSSL**

```
void AES_cbc_encrypt (
    const unsigned char *in,
    unsigned char       *out,
    size_t              length,
    const AES_KEY       *key,
    unsigned char       *ivec,
    AES_ENCRYPT or AES_DECRYPT);
```

**User supplies $IV$**