2550 Intro to cybersecurity

L10: PRF, Block Ciphers

abhi shelat/Ran Cohen

Thanks to Gil Segev (HUJI) for sharing slides

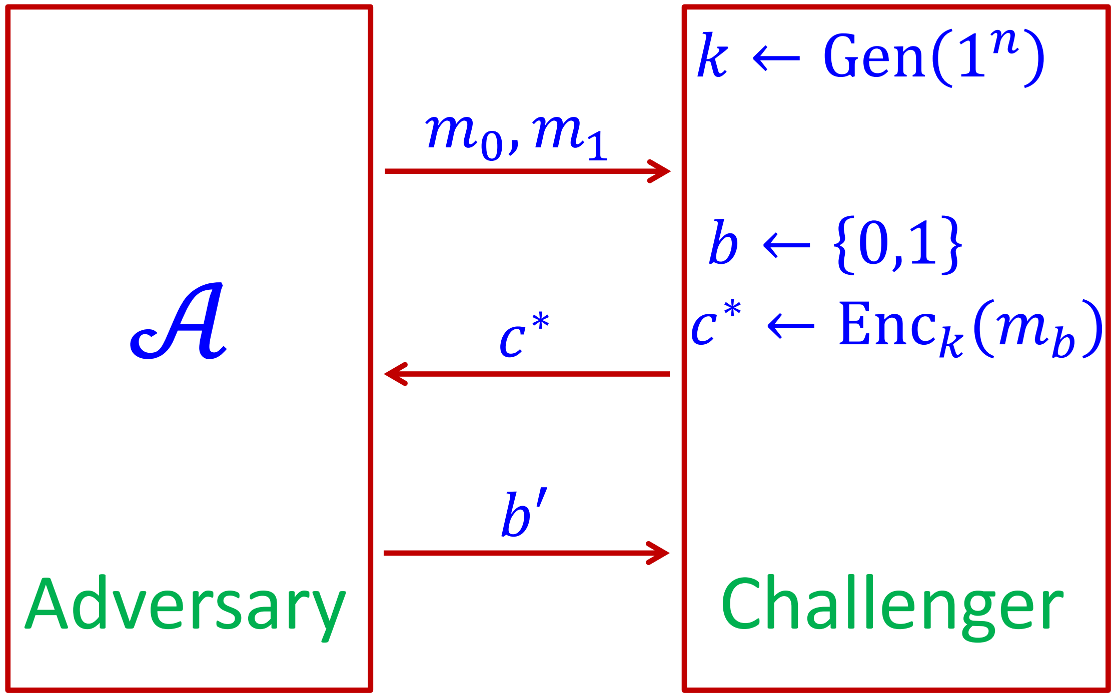
This Week

- Security against a chosen-plaintext attack (CPA)
- Tool: Pseudorandom functions (PRFs)
- CPA-secure encryption from PRFs
- Practical heuristics: Block ciphers
  - Modes of operation

Recall: Indistinguishable Encryptions

Given $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$,
we considered the experiment $\mathrm{IND}_{\Pi,\mathcal{A}}(n)$:

Does this experiment model realistic attacks?

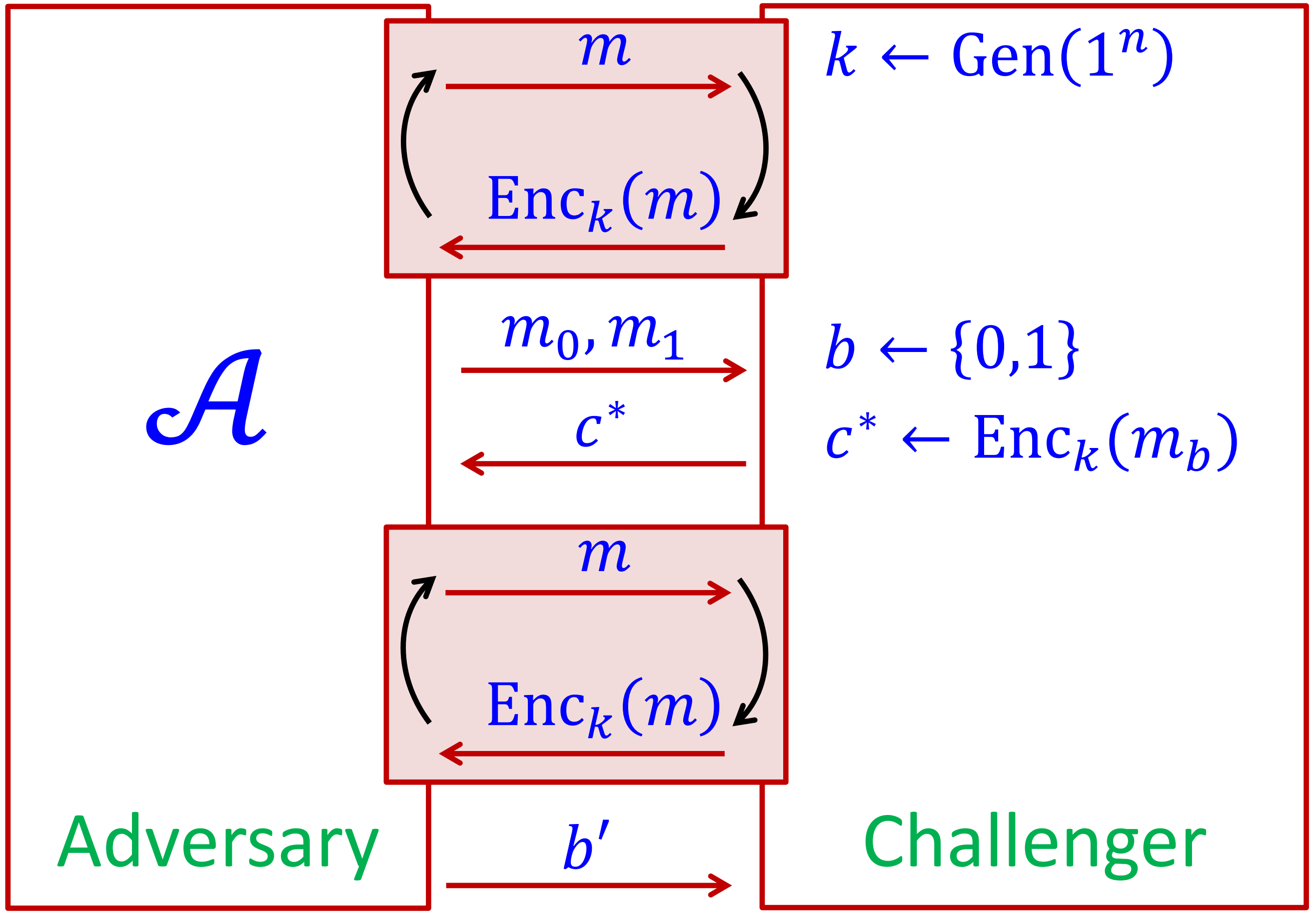


$$\mathrm{IND}_{\Pi,\mathcal{A}}(n) = \begin{cases} 1, & \text{if } b' = b \\ 0, & \text{otherwise} \end{cases}$$

Chosen-Plaintext Attack (CPA)

- Allow $\mathcal{A}$ to ask for any number of encryptions of messages of its choice
- In other words, $\mathcal{A}$ has access to an "encryption oracle" denoted $\mathcal{A}^{\mathrm{Enc}_k(\cdot)}$

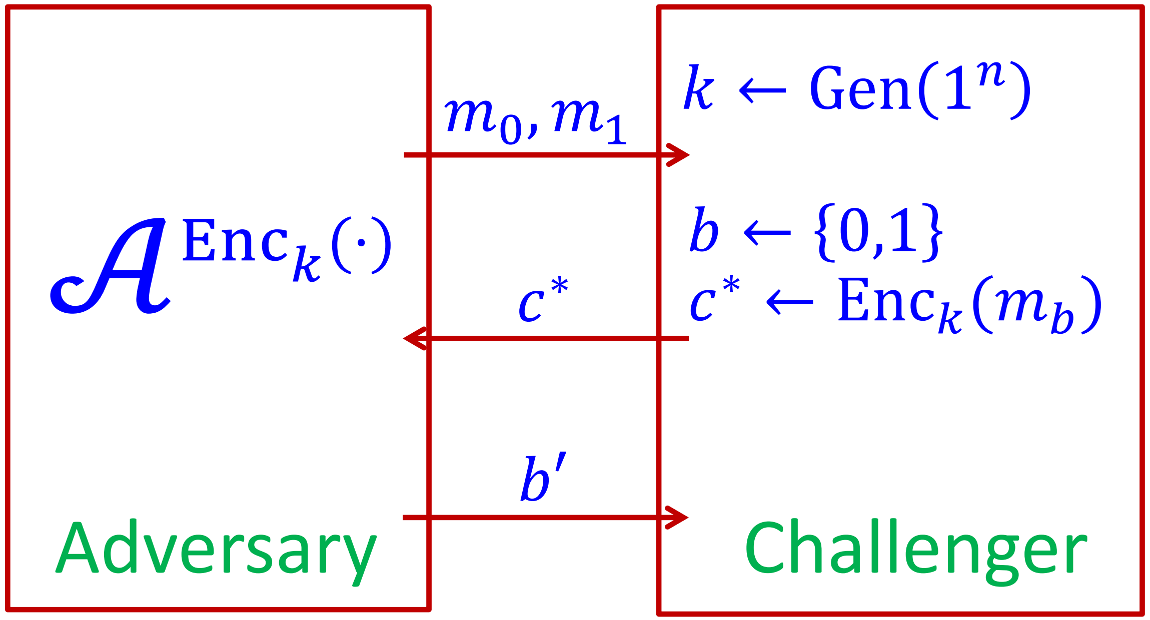
Pythia, the Oracle of Delphi
John Collier, 1891



Chosen-Plaintext Attack (CPA)

Definition:
Π has **indistinguishable encryptions under a chosen-plaintext attack** if for every PPT adversary $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ such that

$$\Pr\left[\mathrm{IND}_{\Pi,\mathcal{A}}^{\mathrm{CPA}}(n) = 1\right] \leq \frac{1}{2} + \nu(n)$$



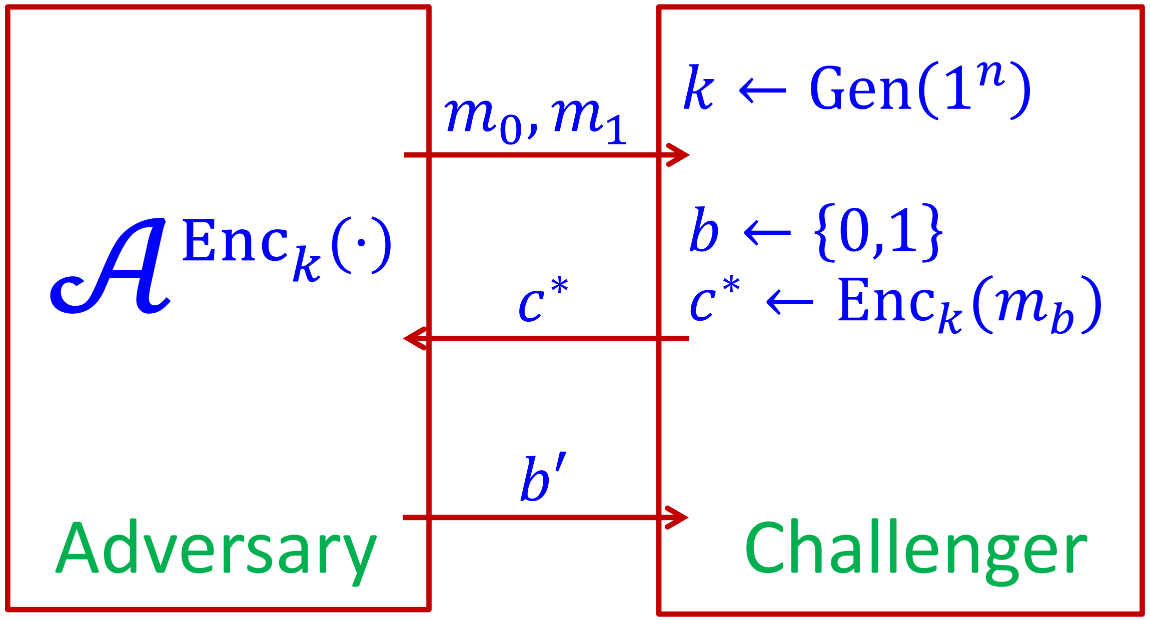
- In short: Π is CPA-secure
- Must use a **randomized** encryption algorithm Enc!
- Implies security for multiple messages

$$\mathrm{IND}_{\Pi,\mathcal{A}}^{\mathrm{CPA}}(n) = \begin{cases} 1, & \text{if } b' = b \\ 0, & \text{otherwise} \end{cases}$$

Chosen-Plaintext Attack (CPA)

Definition:
Π has **indistinguishable encryptions under a chosen-plaintext attack** if for every PPT adversary $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ such that

$$\Pr\left[\mathrm{IND}_{\Pi,\mathcal{A}}^{\mathrm{CPA}}(n) = 1\right] \leq \frac{1}{2} + \nu(n)$$



Is CPA security "too strong"?

- Adversaries may often know, influence or even determine the encrypted content
- CPA security captures all such influences

$$\mathrm{IND}_{\Pi,\mathcal{A}}^{\mathrm{CPA}}(n) = \begin{cases} 1, & \text{if } b' = b \\ 0, & \text{otherwise} \end{cases}$$

CPA Example I

- In May 1942, US Navy cryptanalysts had discovered that Japan was planning an attack on Midway island in the Central Pacific.
- They had learned this by intercepting a communication message containing the ciphertext fragment "AF" that they believed corresponded to the plaintext "Midway island".
- Unfortunately, their attempts to convince Washington planners that this was indeed the case were futile
- The Navy cryptanalysts then devised the following plan. They instructed the US forces at Midway to send a plaintext message that their freshwater supplies were low. The Japanese intercepted this message and reported to their superiors that "AF" was low on water.

CPA Example II

- The cryptanalysts at Bletchley Park would sometimes ask the Royal Air Force to lay mines at specific positions, hoping that the Germans would encrypt a "warning" message and an "all clear" message after they were removed.

- A daily weather report was transmitted by the Germans at the same time every day, containing the word "Wetter" (German for "weather") at the same location in every message.

This Week

- Security against a chosen-plaintext attack (CPA)
- Tool: Pseudorandom functions (PRFs)
- CPA-secure encryption from PRFs
- Practical heuristics: Block ciphers
  - Modes of operation

Pseudorandom Functions (PRFs)

- A pseudorandom function is a function that "looks like" a truly random function
- What is a truly random function?

$$\text{Func}_{n\to\ell} = \text{set of all functions from } \{0,1\}^n \text{ to } \{0,1\}^\ell$$

- $\text{Func}_{2\to1}$: there are $|\{0,1\}|^{|\{0,1\}^2|} = 2^{(2^n)} = 16$ functions from $\{0,1\}^2$ to $\{0,1\}$

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$	$f_9(x)$	$f_{10}(x)$	$f_{11}(x)$	$f_{12}(x)$	$f_{13}(x)$	$f_{14}(x)$	$f_{15}(x)$	$f_{16}(x)$
00	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
01	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
10	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
11	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Pseudorandom Functions (PRFs)

- A pseudorandom function is a function that "looks like" a truly random function
- What is a truly random function?

$$\mathrm{Func}_{n\to\ell} = \text{set of all functions from } \{0,1\}^n \text{ to } \{0,1\}^\ell$$

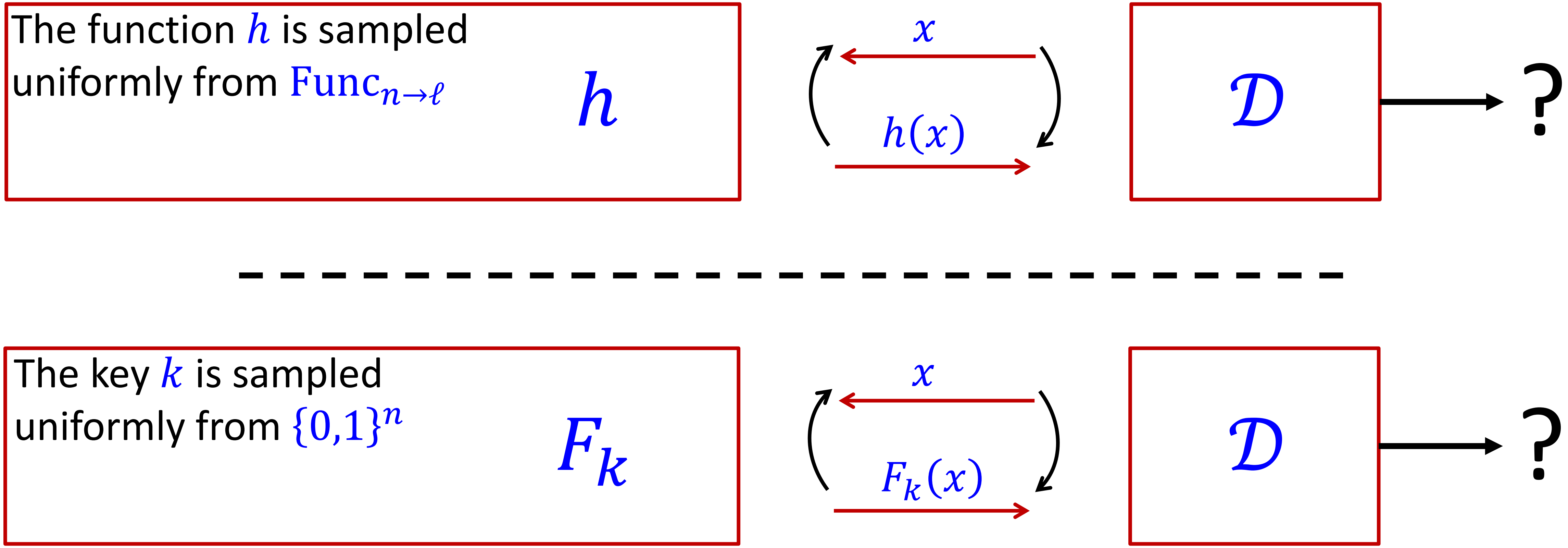
$$|\mathrm{Func}_{n\to\ell}| = \left|\{0,1\}^\ell\right|^{|\{0,1\}^n|} = 2^{\ell\cdot 2^n}$$

- A truly random function is a function h sampled uniformly from $\mathrm{Func}_{n\to\ell}$:
  For each $x \in \{0,1\}^n$ the value $h(x) \in \{0,1\}^\ell$ is chosen uniformly and independently of all other x's

x	$h(x)$
00	01001010
01	00101010
10	11101100
11	10100110

Pseudorandom Functions (PRFs)

A pseudorandom function is an efficiently-computable keyed function $F_k(\cdot): \{0,1\}^n \to \{0,1\}^\ell$ that is computationally indistinguishable from a truly random function



Pseudorandom Functions (PRFs)

Definition (PRF):
An efficiently-computable keyed function $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is **pseudorandom** if for every PPT distinguisher $\mathcal{D}$ there exists a negligible function $\nu(\cdot)$ such that

$$\left|\Pr\left[\mathcal{D}^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[\mathcal{D}^{h(\cdot)}(1^n) = 1\right]\right| \leq \nu(n)$$

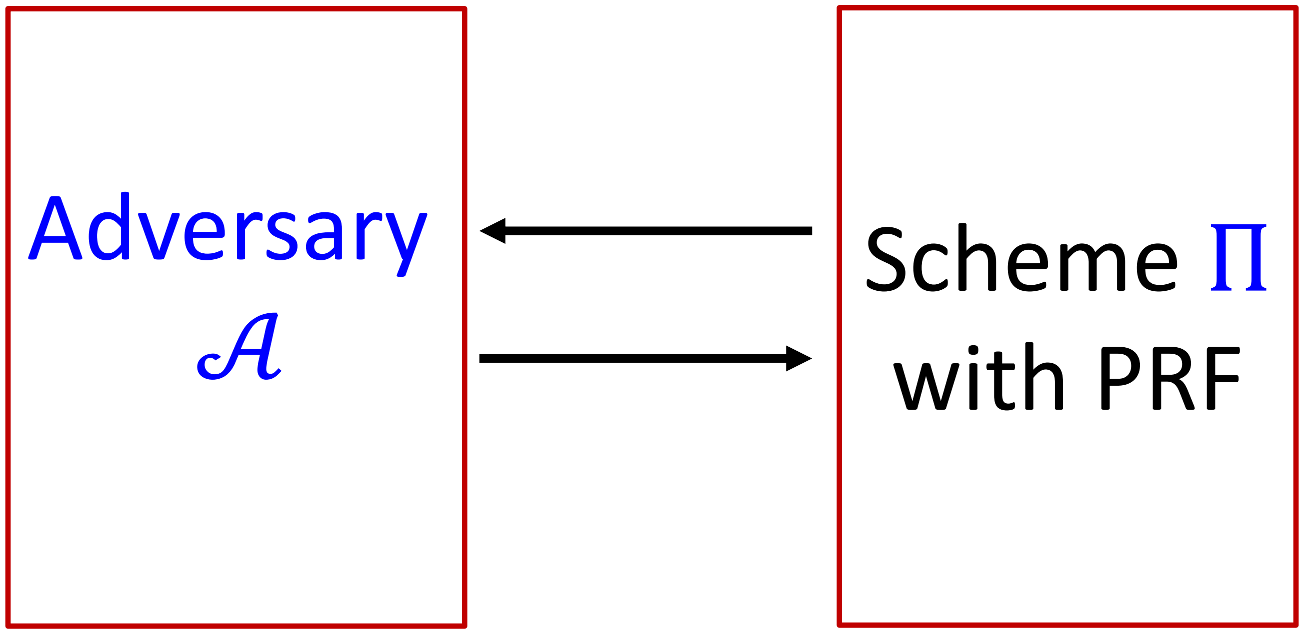
where $k \leftarrow \{0,1\}^n$ and $h \leftarrow \mathrm{Func}_{n\to\ell}$.

Claim (PRF⇒PRG):
Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a PRF, then $G(s) = F_s(1) \cdots F_s(n+1)$ is a PRG

Pseudorandom Functions (PRFs)

The methodology of using PRFs

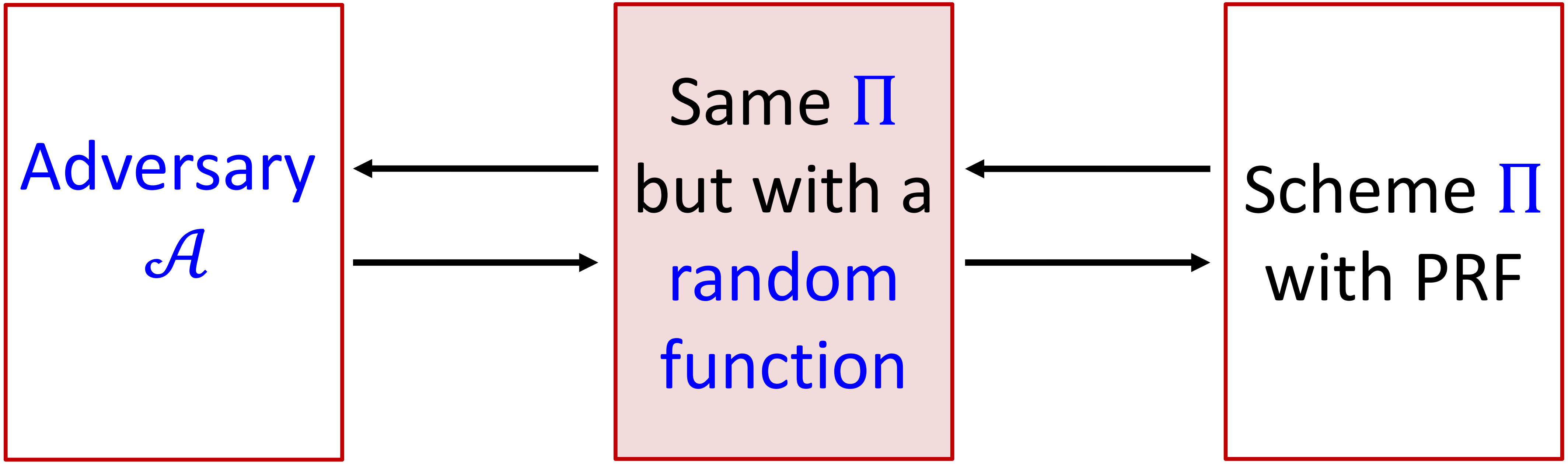
1. Prove security assuming a truly random function is used
2. Prove that if an adversary can break the scheme when PRF is used, then it can be used to distinguish the PRF from a truly random function



Pseudorandom Functions (PRFs)

The methodology of using PRFs

1. Prove security assuming a truly random function is used
2. Prove that if an adversary can break the scheme when PRF is used, then it can be used to distinguish the PRF from a truly random function



This Week

- Security against a chosen-plaintext attack (CPA)
- Tool: Pseudorandom functions (PRFs)
- CPA-secure encryption from PRFs
- Practical heuristics: Block ciphers
  - Modes of operation

CPA-Secure Encryption from PRFs

Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^\ell$ be a PRF

- **Key generation:** Sample $k \leftarrow \{0,1\}^n$
- **Encryption:** On input $k \in \{0,1\}^n$ and $m \in \{0,1\}^\ell$ sample $r \leftarrow \{0,1\}^n$ and output

$$c = (r, F_k(r) \oplus m)$$

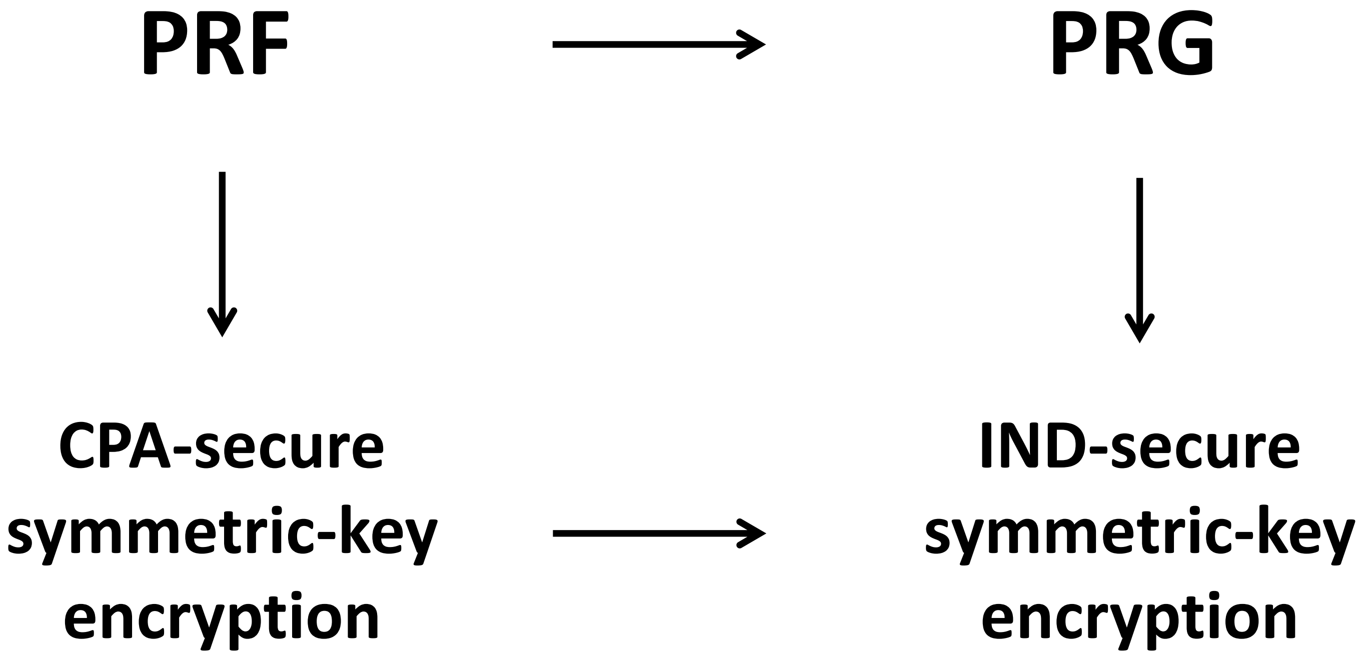
- **Decryption:** On input $k \in \{0,1\}^n$ and $c = (r, s)$ output $m = F_k(r) \oplus s$

Theorem:
If F is a PRF, then the scheme Π_F above is CPA-secure

Proof idea:

- Consider the scheme Π_h that is obtained by using a truly random function h
- The scheme Π_h is (unconditionally) CPA-secure
- The schemes Π_h and Π_F are computationally indistinguishable

The World of Crypto Primitives (so far)



This Week

- Security against a chosen-plaintext attack (CPA)
- Tool: Pseudorandom functions (PRFs)
- CPA-secure encryption from PRFs
- Practical heuristics: Block ciphers
  - Modes of operation

Practical Heuristics: Block Ciphers

- In practice, block ciphers are designed to be secure instantiations of pseudorandom permutations (PRPs)
- A block cipher is an efficiently-computable keyed permutation

$$F: \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$$

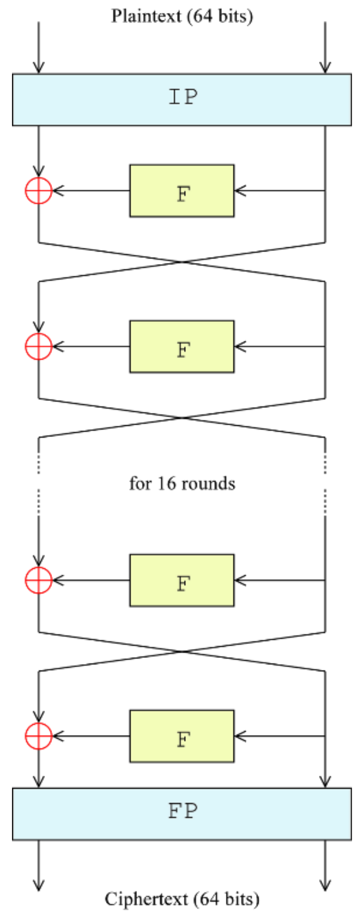
$F_k: \{0,1\}^\ell \to \{0,1\}^\ell$ is a permutation for any key k

- Concrete security rather than asymptotic security
- A block cipher is considered "secure" if the best known "attack" requires time roughly 2^n ($\approx$brute-force search for the key)

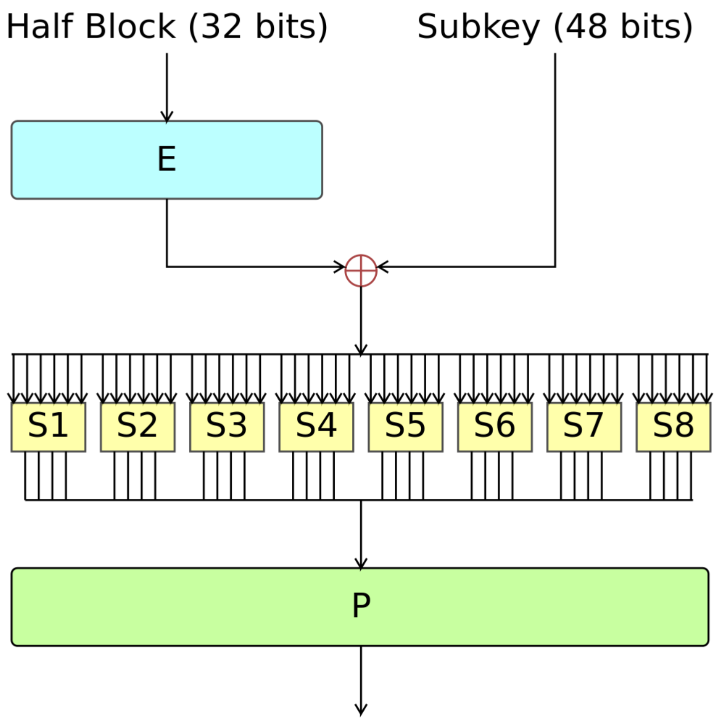
Practical Heuristics: Block Ciphers

DES: The Data Encryption Standard

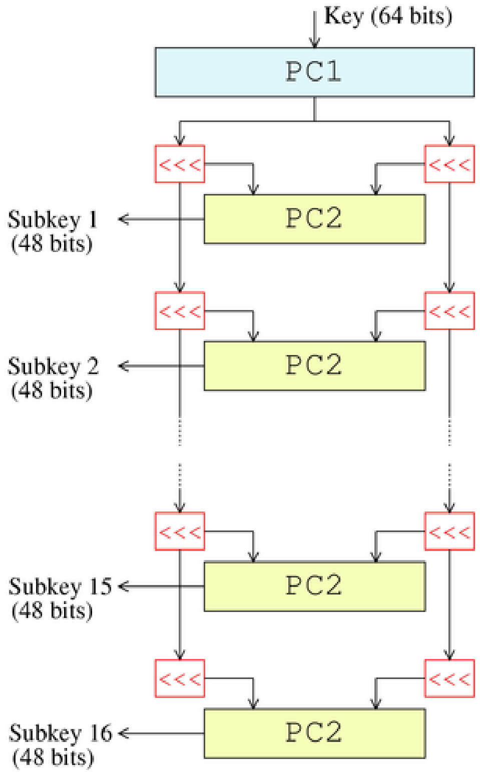
- Developed in the 1970s by IBM (with help from the NSA), adopted in 1977
- Key length is 56 bits, block length is 64 bits



Round function



Key schedule



Practical Heuristics: Block Ciphers

DES: The Data Encryption Standard

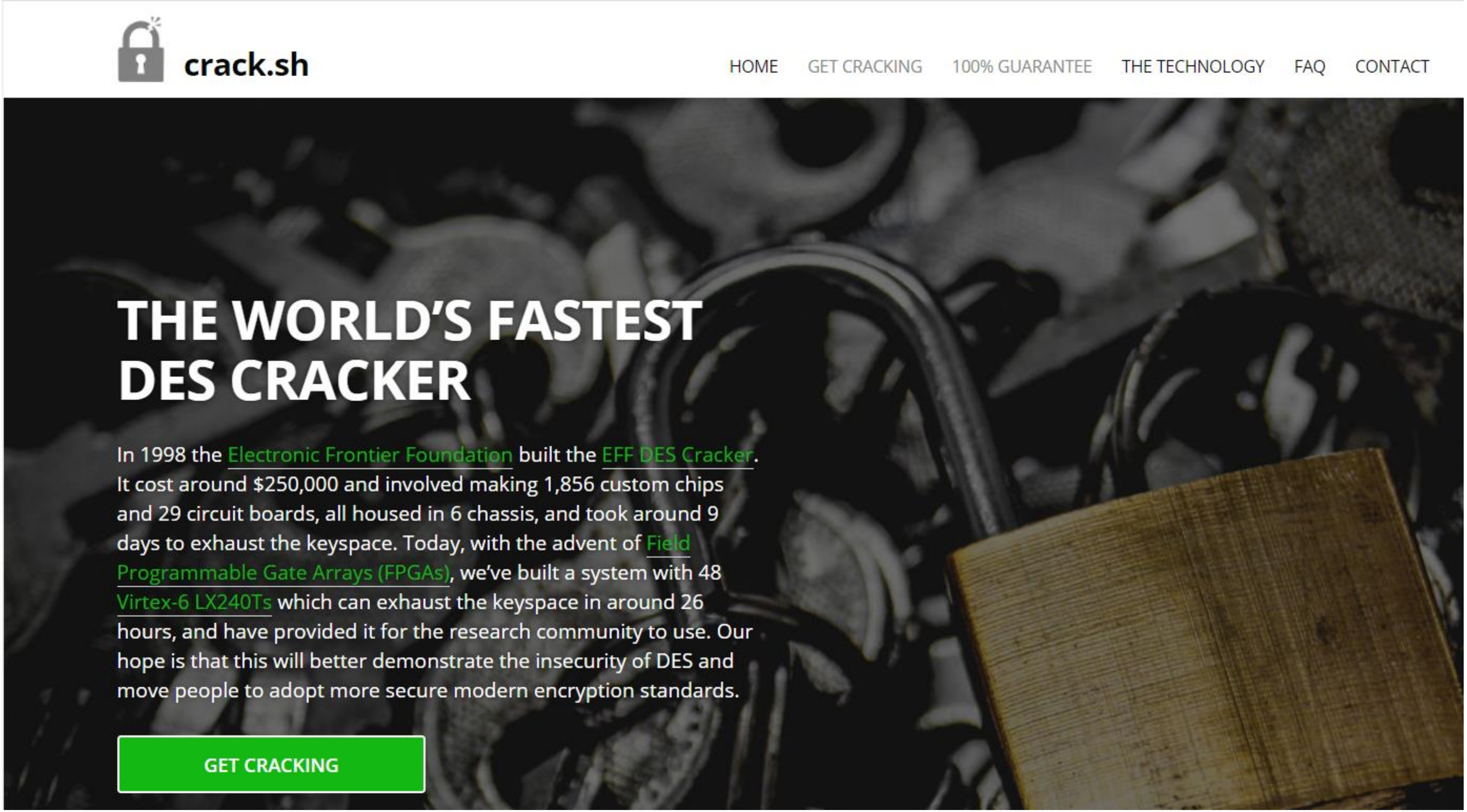
- Developed in the 1970s by IBM (with help from the NSA), adopted in 1977
- Key length is 56 bits, block length is 64 bits
- Best known attack in practice is essentially brute-force key search ($\approx 2^{56}$)
- However, no longer considered secure due to its short key length
- Remains widely-used in the strengthened form of 3DES:

$$3\mathrm{DES}_{k_1,k_2,k_3}(x) = \mathrm{DES}_{k_1}\left(\mathrm{DES}_{k_2}^{-1}\left(\mathrm{DES}_{k_3}(x)\right)\right)$$

3×56-bit keys but can be broken in time $2^{2\times56}$

…and also slower than DES

Practical Heuristics: Block Ciphers



Practical Heuristics: Block Ciphers

AES: The Advanced Encryption Standard

- In 1997 NIST published a call for candidate block ciphers to replace DES
- 15 candidates were proposed by different teams from all over the world
- Each candidate extensively analyzed by the public and by the other teams
- The winner ("Rijndael") was announced in late 2000 (based on security, efficiency, performance in hardware,…)
- Key length is 128/192/256 bits, block length is 128 bits
- To date, no known practical attacks better than brute-force key search

Various design paradigms with insightful structures

Using CPA-Secure Encryption

Recall: CPA-secure encryption from any PRF

$$\mathrm{Enc}_k(m; r) = (r, F_k(r) \oplus m)$$

In practice: AES as a PRF enables to encrypt a 128-bit message

$$\mathrm{Enc}_k(m; r) = (r, \mathrm{AES}_k(r) \oplus m)$$

Why not simply
$\mathrm{Enc}_k(m) = \mathrm{AES}_k(m)$???

Using CPA-Secure Encryption

How to encrypt long messages?

Partition into blocks and use any CPA-secure encryption

$$\mathrm{Enc}_k(m_1 \cdots m_\ell; r_1 \cdots r_\ell)$$
$$= (r_1, F_k(r_1) \oplus m_1), \cdots, (r_\ell, F_k(r_\ell) \oplus m_\ell)$$

In practice: AES as a PRF enables to encrypt 128-bit blocks

$$\mathrm{Enc}_k(m_1 \cdots m_\ell; r_1 \cdots r_\ell)$$
$$= (r_1, \mathrm{AES}_k(r_1) \oplus m_1), \cdots, (r_\ell, \mathrm{AES}_k(r_\ell) \oplus m_\ell)$$

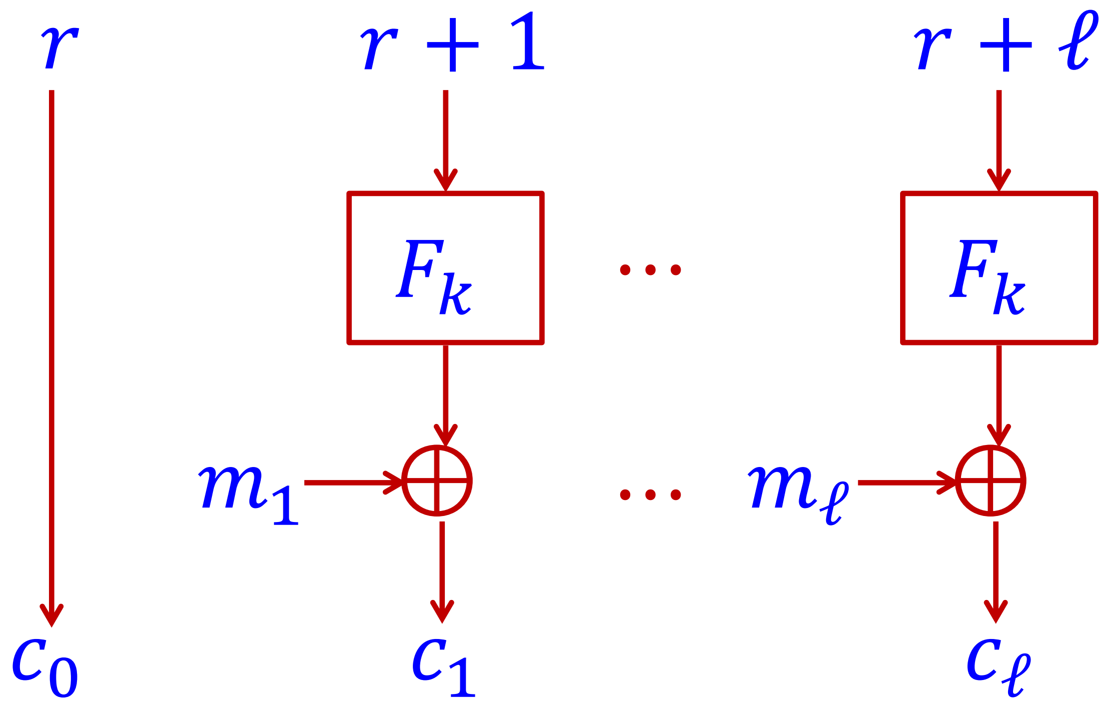
Drawback: Ciphertext length $= 2 \times$ message length

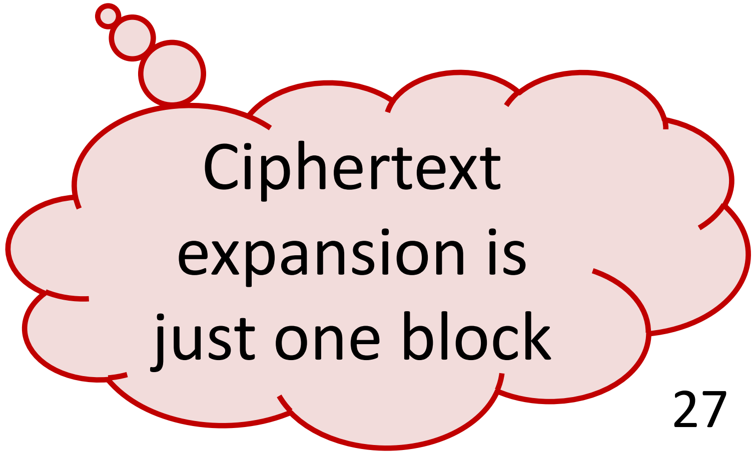
Can we do better?

Modes of Operation

Counter (CTR) mode:

$$\mathrm{Enc}_k(m_1 \cdots m_\ell; r)$$
$$= (r, F_k(r+1) \oplus m_1, F_k(r+2) \oplus m_2, \dots, F_k(r+\ell) \oplus m_\ell)$$





Modes of Operation

Counter (CTR) mode:

$$\text{Enc}_k(m_1 \cdots m_\ell; r)$$
$$= (r, F_k(r+1) \oplus m_1, F_k(r+2) \oplus m_2, \dots, F_k(r+\ell) \oplus m_\ell)$$

Theorem:
If F is a PRF then counter mode is CPA-secure

Proof idea:

- The sequence $s_i = \big(r_i, F_k(r_i+1), \dots, F_k(r_i+\ell)\big)$ used for encrypting the ith message is pseudorandom

Modes of Operation

- Several other useful and secure modes of operations
- e.g., CBC (cipher block chaining) and OFB (output feedback)

Electronic CodeBook (ECB) mode:

$$\text{Enc}_k(m_1 \cdots m_\ell) = \left(F_k(m_1), F_k(m_2), \ldots, F_k(m_\ell)\right)$$

- Deterministic and thus not CPA secure
- Does not even have indistinguishable encryptions
  - E.g., $m_0 = 0^n 0^n$ and $m_1 = 0^n 1^n$

Assuming F_k is efficiently invertible given k (e.g., AES)

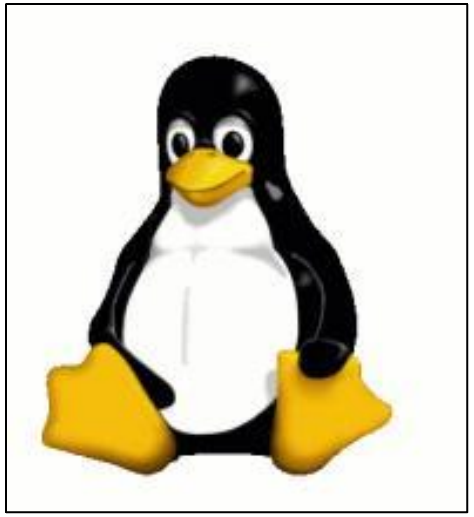
Modes of Operation

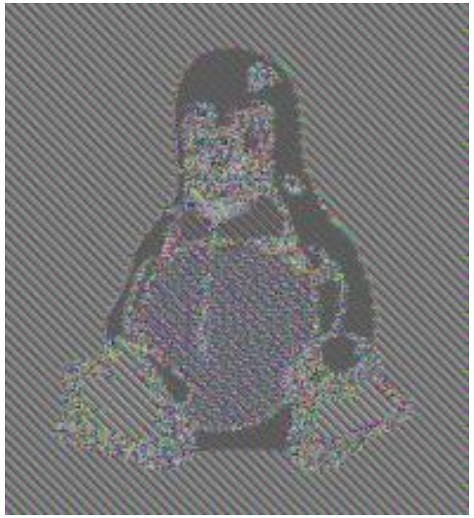
- Several other useful and secure modes of operations
- e.g., CBC (cipher block chaining) and OFB (output feedback)

Electronic CodeBook (ECB) mode:

$$\mathrm{Enc}_k(m_1 \cdots m_\ell) = \left(F_k(m_1), F_k(m_2), \ldots, F_k(m_\ell)\right)$$

Original image





ECB mode encryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation