Block Ciphers and CPA Security

CS/ECE 407

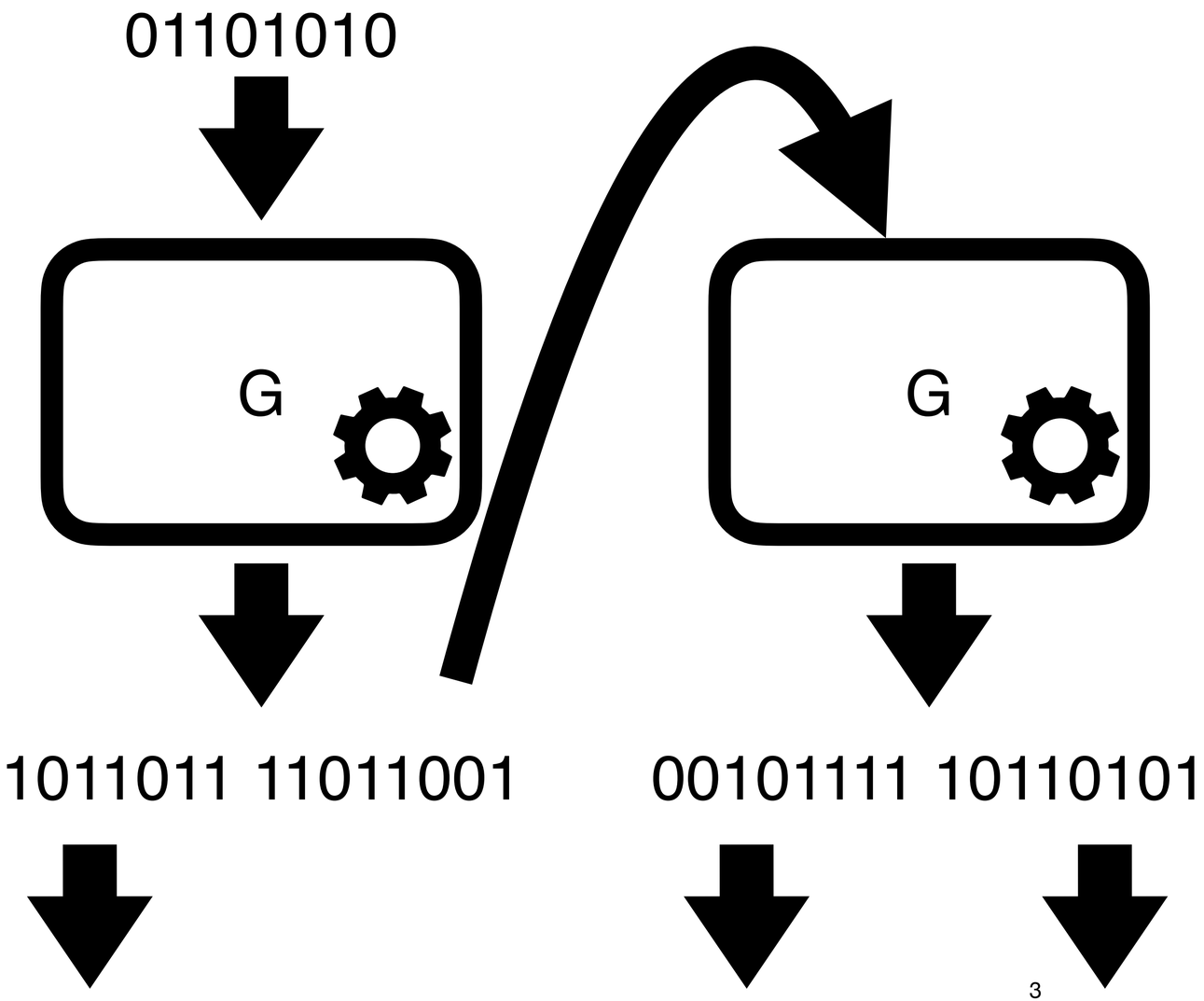
Today’s objectives

Define block ciphers

Introduce CPA Security

Understand the limitations of deterministic encryption

Stretching the output of a PRG



Call multiple times to get more randomness

What about a cryptographic primitive that generates a lot of randomness “all at once”

Alice

Bob

2^n **rows**

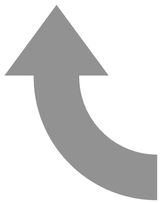
0	01101000
1	11110000
2	10001110
3	01010100
4	11011010
…	…

A pseudorandom function (PRF) allows Alice and Bob to share a huge pseudorandom table via a short key

$$F : \{0,1\}^{\lambda} \times \{0,1\}^{n} \rightarrow \{0,1\}^{m}$$

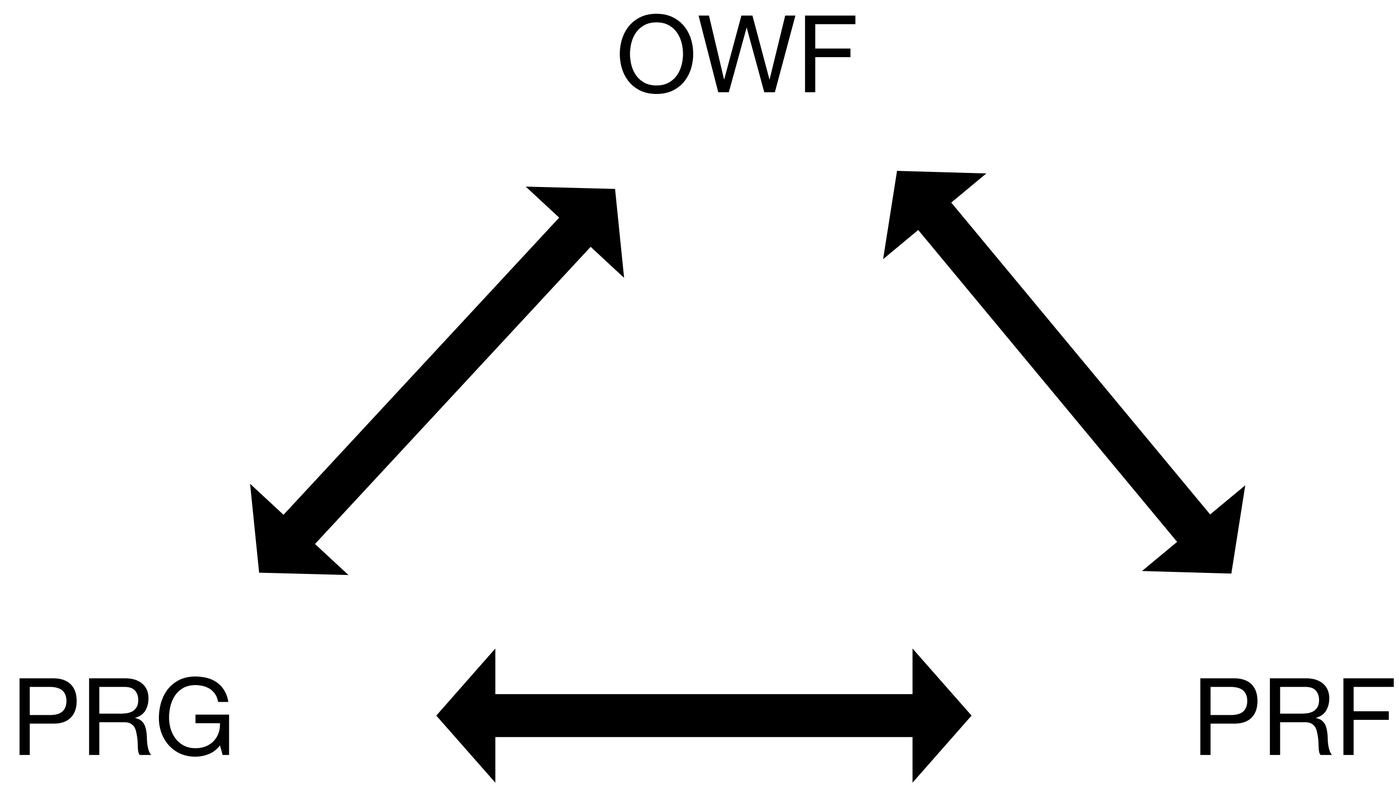
F is called a **pseudorandom function family** if the following indistinguishability holds:

$$\left\{ F(k, \cdot) \;\middle|\; k \leftarrow \{0,1\}^{\lambda} \right\} \approx \left\{ f \;\middle|\; f \leftarrow \text{uniform function from } \{0,1\}^{n} \rightarrow \{0,1\}^{m} \right\}$$



Uniformly sampling k “emulates” a huge random table

Closer to how many real-world primitives are defined

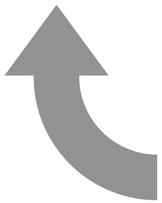


OWFs exist $\Longrightarrow$ $P \neq NP$

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

F is called a **pseudorandom function family** if the following indistinguishability holds:

$$\left\{ F(k, \cdot) \;\middle|\; k \leftarrow \{0,1\}^{\lambda} \right\} \approx \left\{ f \;\middle|\; f \leftarrow \text{uniform function from } \{0,1\}^{n} \to \{0,1\}^{m} \right\}$$



Uniformly sampling k “emulates” a huge random table

Closer to how many real-world primitives are defined

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

F is called a **pseudorandom permutation (or block cipher)** if:

$$\left\{ F(k, \cdot) \;\middle|\; k \leftarrow \{0,1\}^\lambda \right\}$$

$$\approx$$

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform permutation from } \{0,1\}^n \to \{0,1\}^n \right\}$$

And there exists efficient F^{-1} s.t. $F^{-1}(k, F(k, x)) = x$

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

Block length

F is called a **pseudorandom permutation (or block cipher)** if:

$$\left\{ F(k, \cdot) \;\middle|\; k \leftarrow \{0,1\}^{\lambda} \right\}$$

$$\approx$$

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform permutation from } \{0,1\}^{n} \to \{0,1\}^{n} \right\}$$

And there exists efficient F^{-1} s.t. $F^{-1}(k, F(k, x)) = x$

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

Block length

F is called a **pseudorandom permutation (or block cipher)** if:

$$\left\{ F(k, \cdot) \;\middle|\; k \leftarrow \{0,1\}^{\lambda} \right\}$$

$$\approx$$

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform permutation from } \{0,1\}^{n} \to \{0,1\}^{n} \right\}$$

And there exists efficient F^{-1} s.t. $F^{-1}(k, F(k, x)) = x$

AES is a block cipher

Every PRP with large block length is a PRF

“Switching Lemma”

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform permutation from } \{0,1\}^\lambda \to \{0,1\}^\lambda \right\}$$

$$\approx$$

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform function from } \{0,1\}^\lambda \to \{0,1\}^\lambda \right\}$$

Every PRP with large block length is a PRF

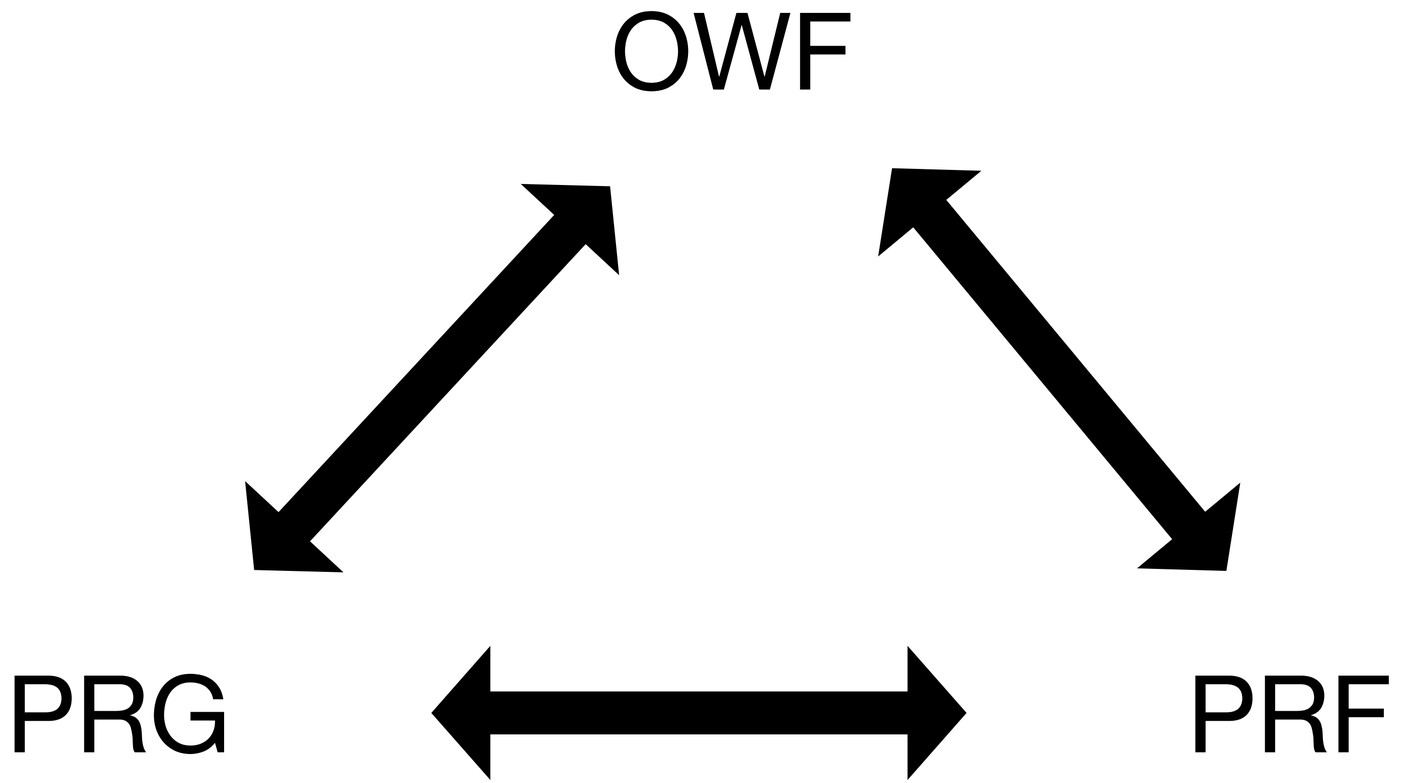
"Switching Lemma"

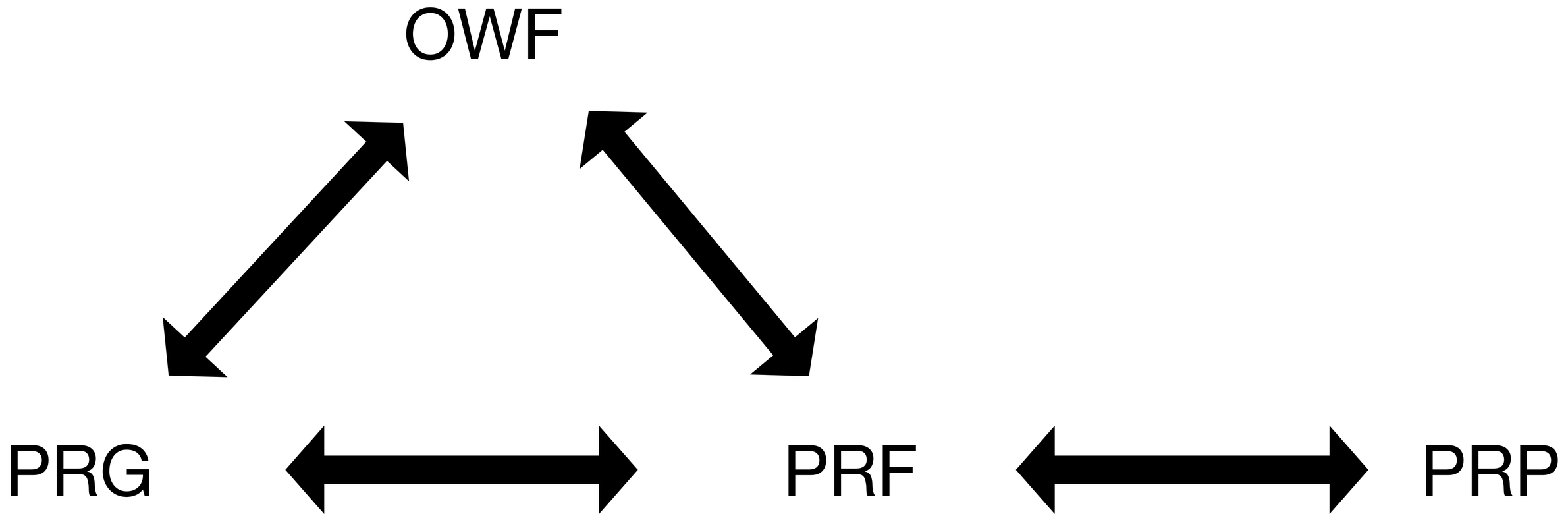
$$\left\{ f \;\middle|\; f \leftarrow \text{uniform permutation from } \{0,1\}^\lambda \to \{0,1\}^\lambda \right\}$$

$$\approx$$

$$\left\{ f \;\middle|\; f \leftarrow \text{uniform function from } \{0,1\}^\lambda \to \{0,1\}^\lambda \right\}$$

Intuition: only way to distinguish is to find a collision in function f, but collisions are rare, so polytime adversary does not have time to find one

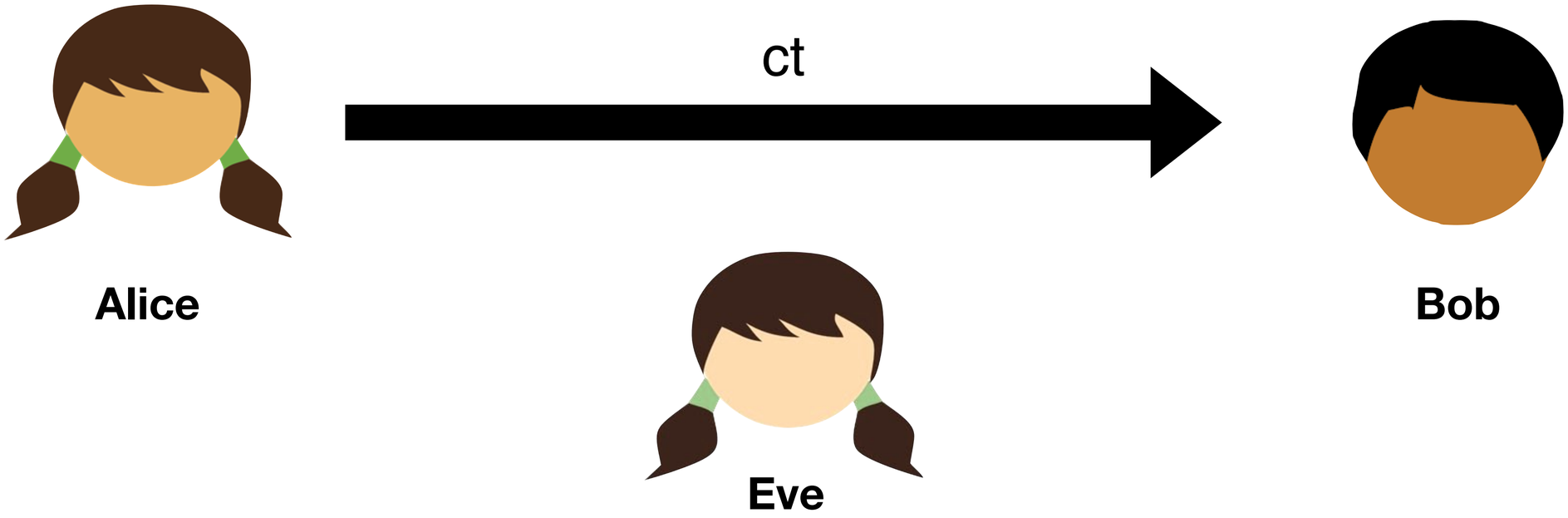

OWF
PRG
PRF


OWF
PRG
PRF
PRP

A cipher (Enc, Dec) has **one-time security** if:

For every message $m \in \mathrm{M}$:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow K \\ c = Enc(k, m) \end{array} \right\} \approx \left\{ c \;\middle|\; c \leftarrow C \right\}$$

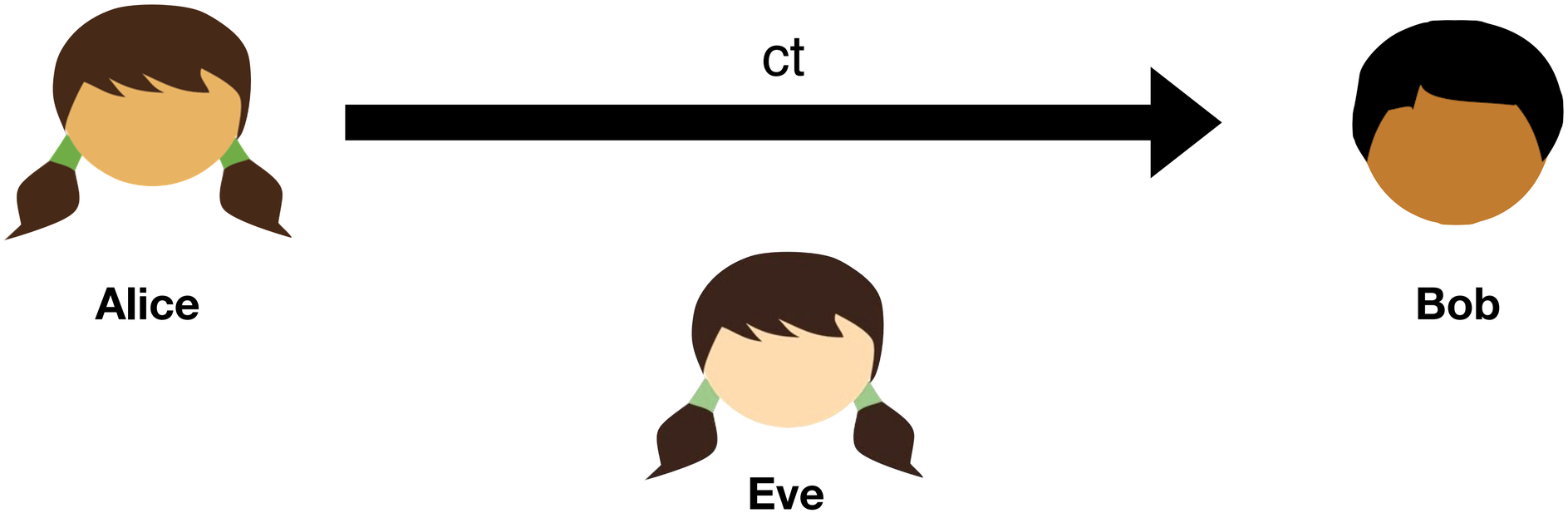


A cipher (Enc, Dec) has **one-time security** if:

For every message $m \in \mathrm{M}$:

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow K \\ c = Enc(k, m) \end{array} \right\} \approx \left\{ c \;\middle|\; c \leftarrow C \right\}$$

How can we implement (Enc, Dec) with a block cipher?



A cipher (Enc, Dec) has **one-time security** if:

For every message $m \in \mathrm{M}$:

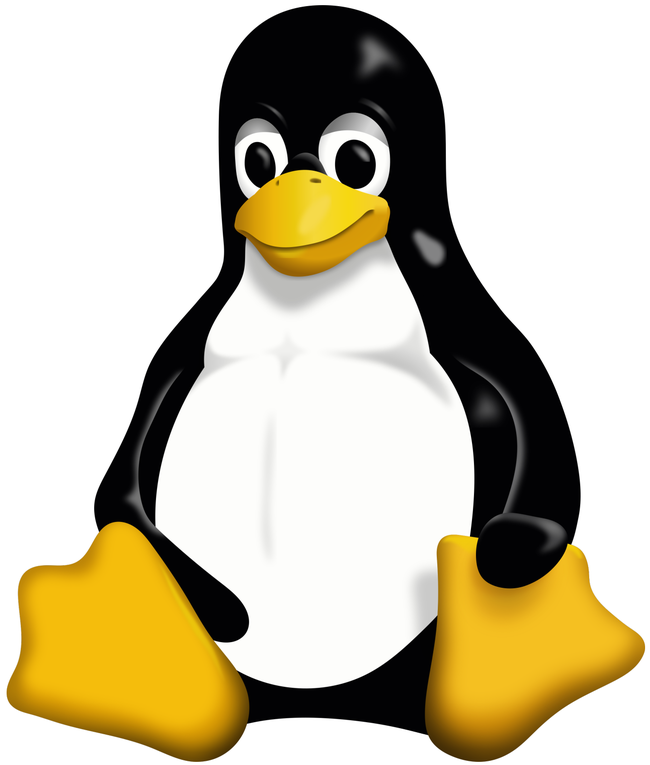
$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow K \\ c = Enc(k, m) \end{array} \right\} \approx \left\{ c \;\middle|\; c \leftarrow C \right\}$$

What if Alice/Bob want to exchange more than one message?

Deterministic Encryption

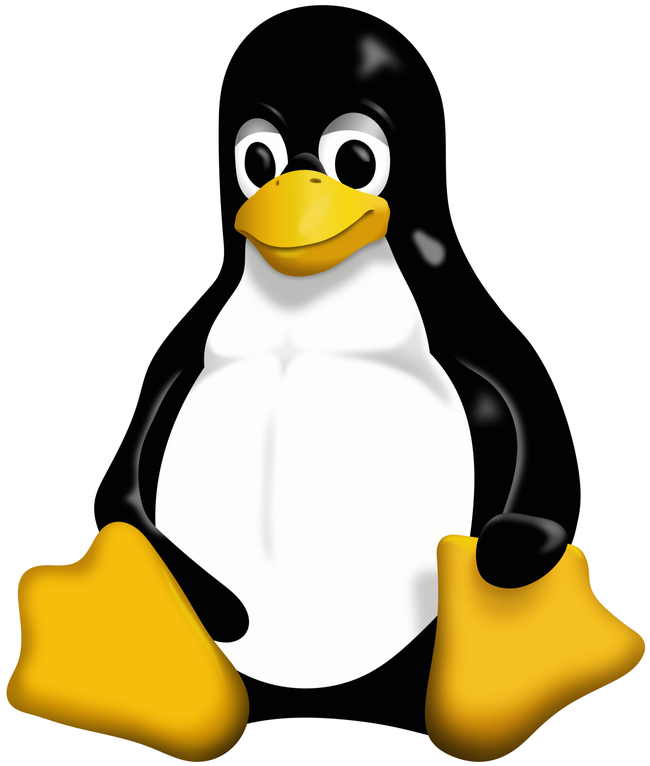
A cipher (Enc, Dec) is **deterministic** if calling $Enc(k, m)$ on the same inputs twice always produces the same output

Deterministic Encryption is (often) Bad



“Tux”

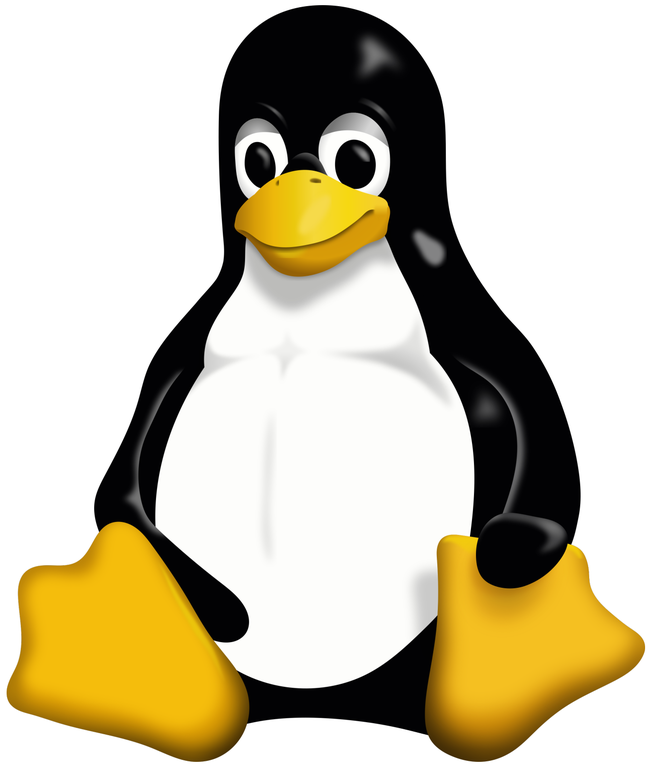
Deterministic Encryption is (often) Bad



"Tux"

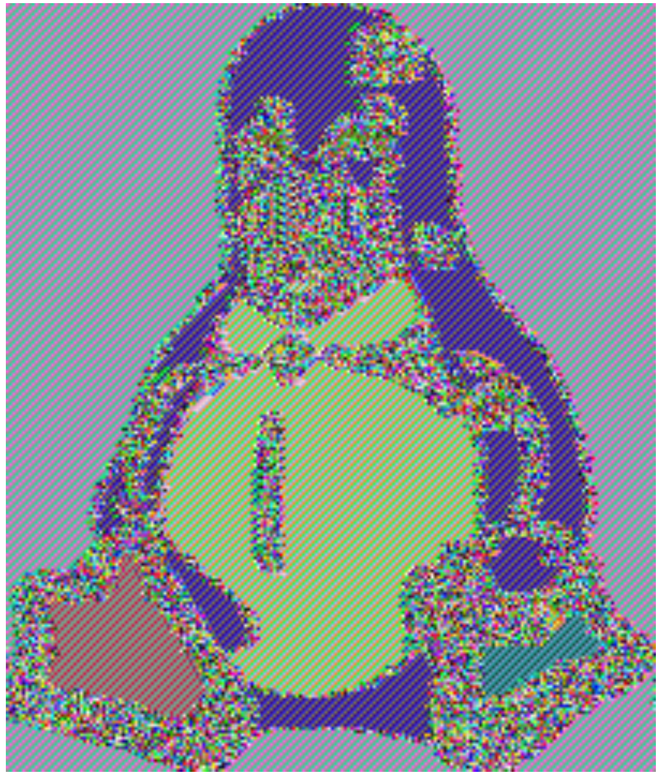
"Good" encryption

Deterministic Encryption is (often) Bad



"Tux"

"Good" encryption



Deterministic Encryption

A cipher (Enc, Dec) has **ciphertext indistinguishability against a chosen plaintext attack (CPA)** if:

Let $Enc_L(k, m_0, m_1) = Enc(k, m_0)$

Let $Enc_R(k, m_0, m_1) = Enc(k, m_1)$

Where m_0, m_1 are of the same length

A cipher (Enc, Dec) has **ciphertext indistinguishability against a chosen plaintext attack (CPA)** if:

Let $Enc_L(k, m_0, m_1) = Enc(k, m_0)$

Let $Enc_R(k, m_0, m_1) = Enc(k, m_1)$

Where m_0, m_1 are of the same length

$$\left\{ Enc_L(k, \cdot, \cdot) \;\middle|\; k \leftarrow K \right\} \approx \left\{ Enc_R(k, \cdot, \cdot) \;\middle|\; k \leftarrow K \right\}$$

A cipher (Enc, Dec) has **random ciphertexts against a chosen plaintext attack (CPA$)** if:

$$Samp(m) = \{c \mid c \leftarrow C(|m|)\}$$

Ciphertext of length corresponding to message m

$$\{Enc(k, \cdot) \mid k \leftarrow K\} \approx Samp(\cdot)$$

In order to achieve CPA security a cipher must not be deterministic

Randomized CPA-Secure Encryption

```
Enc(k, m):
  r ←{0,1}^λ
  c0 = F(k, r) ⊕ m
  c = (c0, r)
  return c

Dec(k, (c0, r)):
  return F(k, r) ⊕ c0
```

Main idea: it is unlikely that Enc will sample the same r more than once

Proof of security is more nuanced here

Today's objectives

Define block ciphers

Introduce CPA Security

Understand the limitations of deterministic encryption