One-time Secure Encryption; PRFs and OWFs

CS/ECE 407

Today’s objectives

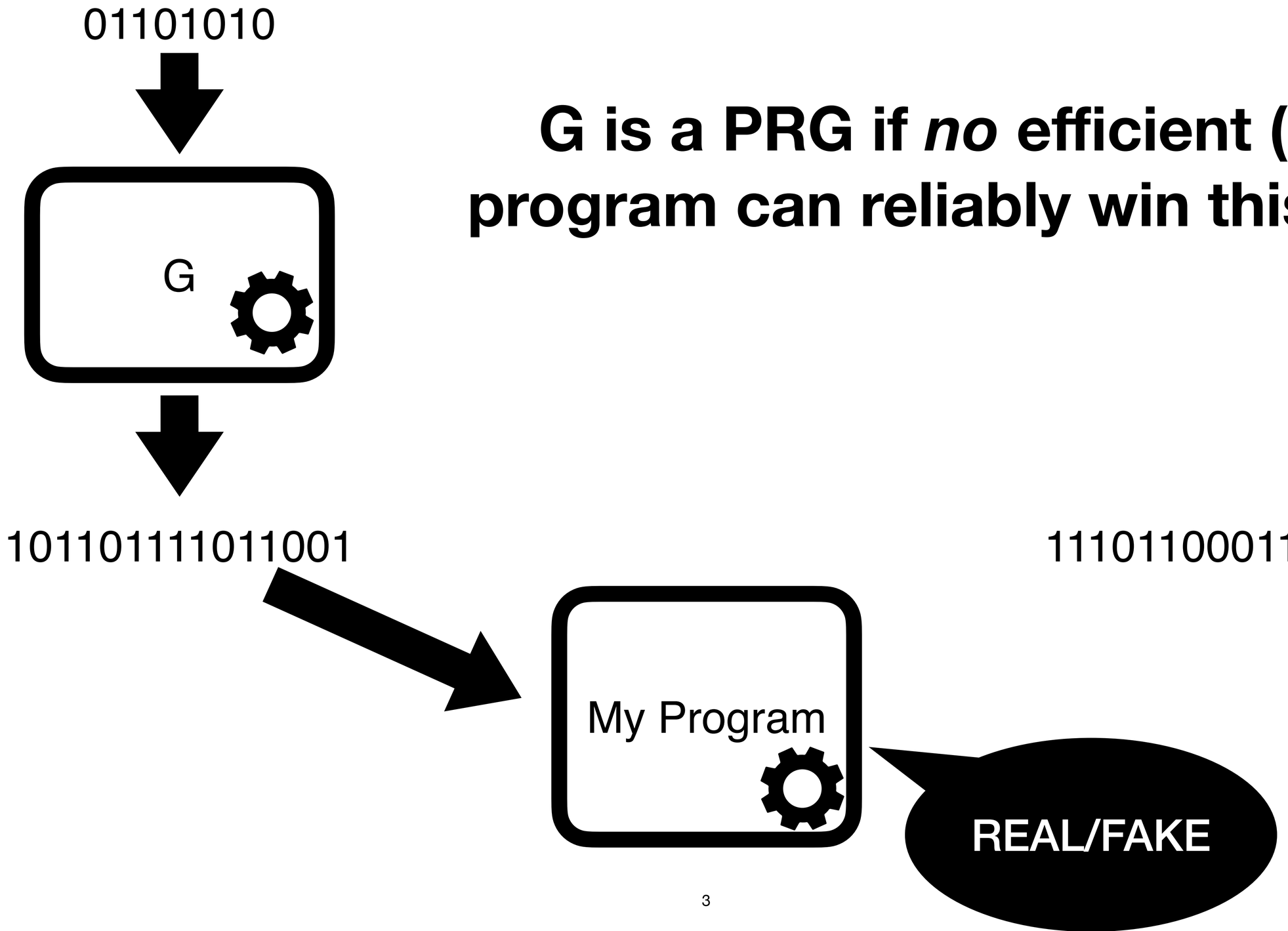
Use PRG to define a new cipher

Define one-time secure cipher

Prove our cipher satisfies one-time security

Introduce Pseudorandom Functions (PRFs) and one-way functions

Discuss connections between PRGs, PRFs, OWFs



G is a PRG if *no* efficient (PPT) program can reliably win this game

Indistinguishability

Let X, Y be two probability ensembles, and let A be an arbitrary (probabilistic) program that outputs 0 or 1. A's **advantage** is as follows:

$$\text{Advantage}_A(\lambda) = \left| \Pr\left[b = 1 \;\middle|\; \begin{array}{l} x \leftarrow_{\$} X_\lambda \\ b \leftarrow A(1^\lambda, x) \end{array} \right] - \Pr\left[b = 1 \;\middle|\; \begin{array}{l} y \leftarrow_{\$} Y_\lambda \\ b \leftarrow A(1^\lambda, y) \end{array} \right] \right|$$

We say that X, Y are **indistinguishable,** written $X \approx Y$ if for every polynomial-time program A:

$\text{Advantage}_A(\lambda)$ is negligible

best strategy is only negligibly better than guessing

PRG security

Let G be a poly-time deterministic algorithm that on an input of length λ outputs a string of length $\lambda + s(\lambda)$.
G is a PRG if $s(\lambda)$ is always positive, and:

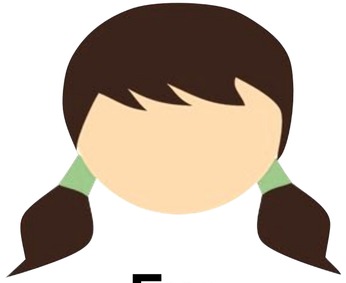
$$\left\{ G(k) \;\middle|\; k \leftarrow \{0,1\}^{\lambda} \right\} \approx \left\{ r \;\middle|\; r \leftarrow \{0,1\}^{\lambda+s(\lambda)} \right\}$$

"If seed k is uniform and hidden, then $G(k)$ looks uniform"

$k \leftarrow \{0,1\}^n$

ct

Alice



Eve

Bob

$m \in \{0,1\}^n$

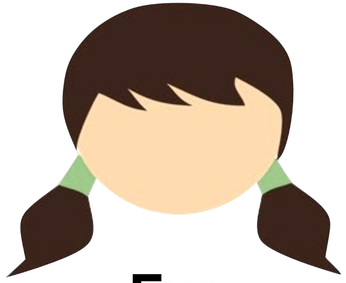
$ct \leftarrow m \oplus k$

$m \leftarrow ct \oplus k$

$k \leftarrow \{0,1\}^n$

ct

Alice



Eve

Bob

$m \in \{0,1\}^n$

$ct \leftarrow m \oplus k$

$m \leftarrow ct \oplus k$

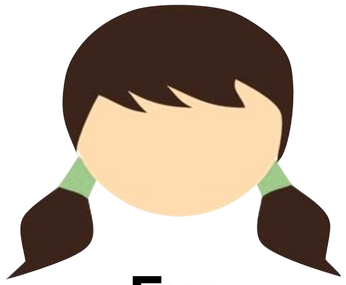
Perfect Secrecy: For every message $m \in \mathrm{M}$:

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

Alice

$s \leftarrow \{0,1\}^{\lambda}$

ct



Eve

Bob

$m \in \{0,1\}^{n}$

$k \leftarrow G(s)$

$ct \leftarrow m \oplus k$

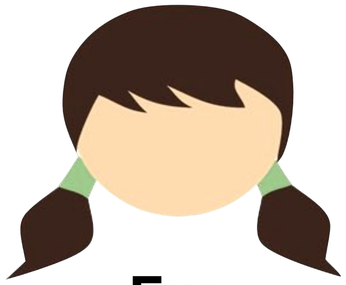
$k \leftarrow G(s)$

$m \leftarrow ct \oplus k$

$s \leftarrow \{0,1\}^{\lambda}$

ct

Alice



Eve

Bob

$m \in \{0,1\}^{n}$

$k \leftarrow G(s)$

$ct \leftarrow m \oplus k$

$k \leftarrow G(s)$

$m \leftarrow ct \oplus k$

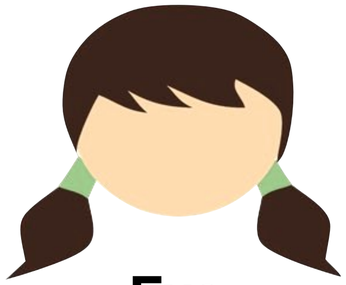
Security?

Alice

$s \leftarrow \{0,1\}^{\lambda}$

ct

Bob



Eve

$m \in \{0,1\}^{n}$

$k \leftarrow G(s)$

$ct \leftarrow m \oplus k$

$k \leftarrow G(s)$

$m \leftarrow ct \oplus k$

Perfect Secrecy:

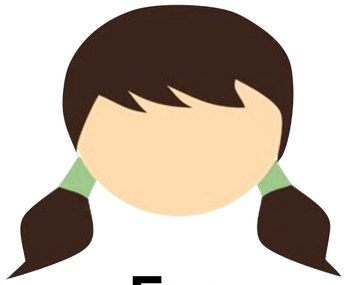
For every message $m \in \mathrm{M}$:

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

$s \leftarrow \{0,1\}^\lambda$

ct

Alice



Eve

Bob

$m \in \{0,1\}^n$

$k \leftarrow G(s)$

$ct \leftarrow m \oplus k$

$k \leftarrow G(s)$

$m \leftarrow ct \oplus k$

Perfect Secrecy:

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

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

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

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

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

Perfect Secrecy:

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

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

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = Enc(k, m) \end{array} \right\}$$

$$\left\{ c \;\middle|\; c \leftarrow \{0,1\}^{n} \right\}$$

For every message $m \in \{0,1\}^n$

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = Enc(k,m) \end{array} \right\}$$

Goal

$$\approx$$

$$\left\{ c \;\middle|\; c \leftarrow \{0,1\}^{n} \right\}$$

For every message $m \in \{0,1\}^n$

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = Enc(k, m) \end{array} \right\}$$

$$\equiv \qquad \text{Defn. Enc}$$

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = G(k) \oplus m \end{array} \right\}$$

$$\left\{ c \;\middle|\; c \leftarrow \{0,1\}^{n} \right\}$$

For every message $m \in \{0,1\}^n$

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = Enc(k, m) \end{array} \right\}$$

$$\equiv$$

Defn. Enc

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = G(k) \oplus m \end{array} \right\}$$

PRG Security

$$\approx$$

$$\left\{ c \;\middle|\; c \leftarrow \{0,1\}^{n} \right\}$$

$$\left\{ c \;\middle|\; \begin{array}{l} r \leftarrow \{0,1\}^{n} \\ c = r \oplus m \end{array} \right\}$$

For every message $m \in \{0,1\}^n$

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = Enc(k,m) \end{array} \right\}$$

$\equiv$ **Defn. Enc**

$$\left\{ c \;\middle|\; \begin{array}{l} k \leftarrow \{0,1\}^{\lambda} \\ c = G(k) \oplus m \end{array} \right\}$$

PRG Security

$\approx$

$$\left\{ c \;\middle|\; c \leftarrow \{0,1\}^{n} \right\}$$

Perfect Secrecy of one-time pad

$\equiv$

$$\left\{ c \;\middle|\; \begin{array}{l} r \leftarrow \{0,1\}^{n} \\ c = r \oplus m \end{array} \right\}$$

For every message $m \in \{0,1\}^{n}$

$s \leftarrow \{0,1\}^{\lambda}$

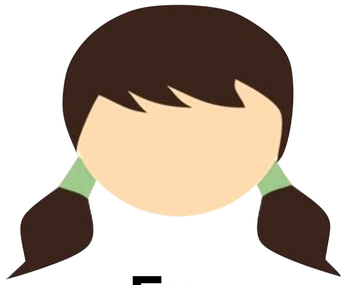
ct

Alice

$m \in \{0,1\}^n$

$k \leftarrow G(s)$

$ct \leftarrow m \oplus k$



Eve

Bob

$k \leftarrow G(s)$

$m \leftarrow ct \oplus k$

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

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

Messages look random to poly-time Eve

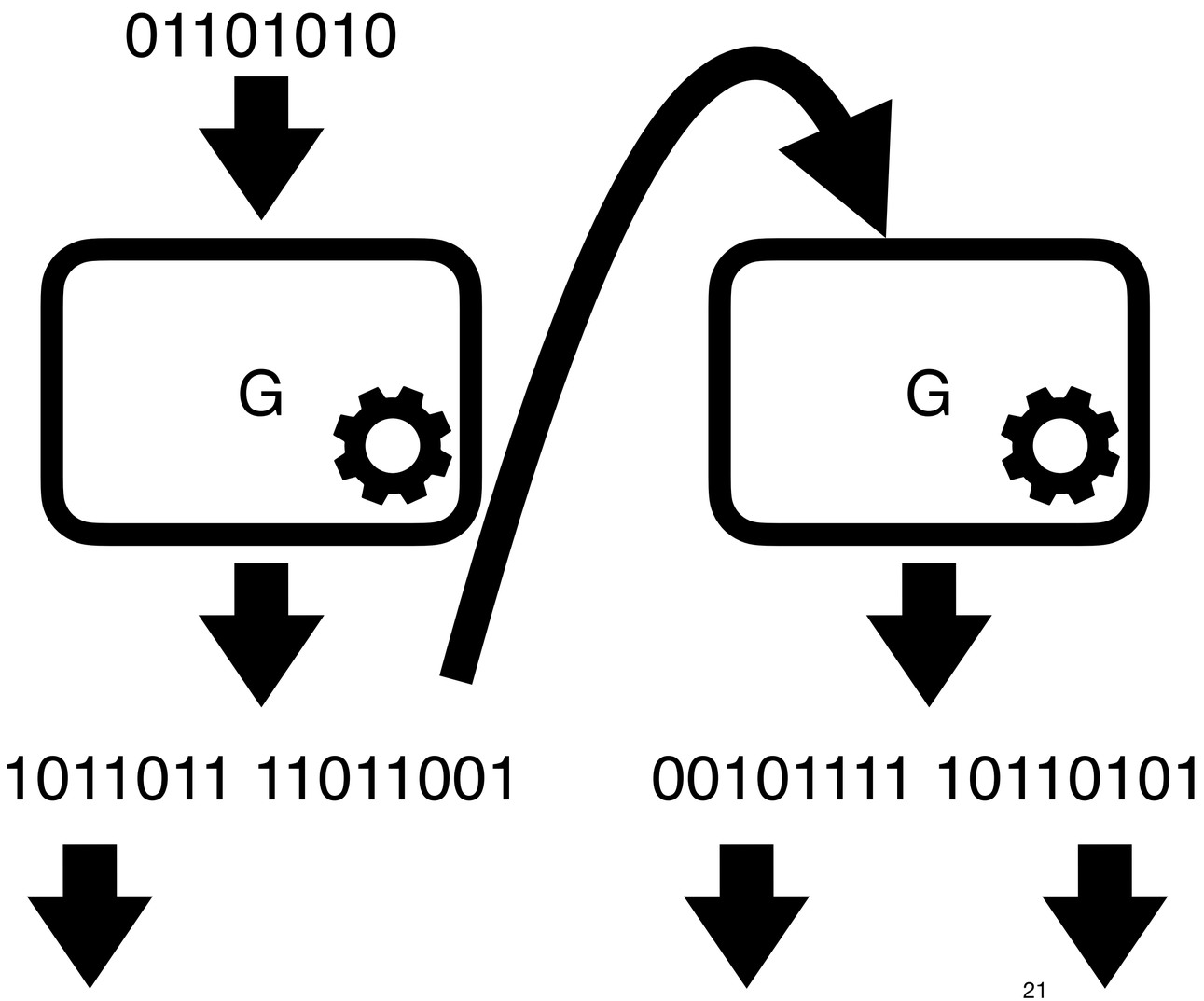
Now, Alice can send one long message to Bob, using only a short key

From here…
- **More than one message?**
- **Authenticity?**

We will introduce new tools to get these

Pseudorandom Functions

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

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

Bob

Alice

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

Bob

2^{λ} **rows**

Alice

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

Bob

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

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

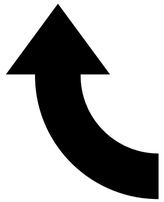
F is called a **pseudorandom function family** if the following indistinguishability holds:

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

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

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

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

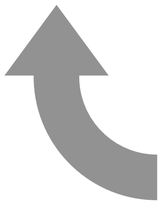


The adversary gets black-box access (or *oracle access*) to the function

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

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

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

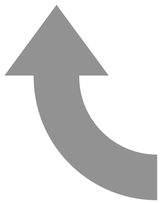


Uniformly sampling k “emulates” a huge random table

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

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

Advanced Encryption Standard

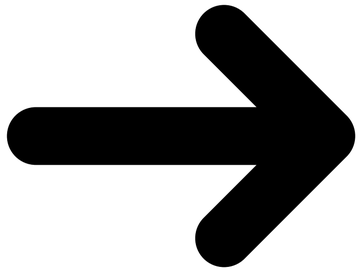
Designed by Joan Daemen and Vincent Rijmen

Adopted by National Institute of Standards and Technology (NIST) in 2001, as winner of long contest

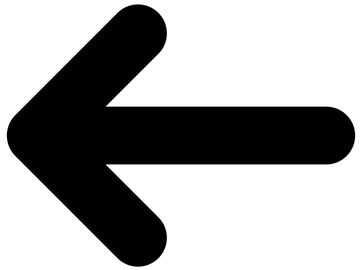
Just “mixes up bits”

Built into the hardware of just about every modern computer and phone

Given a PRF, build a PRG



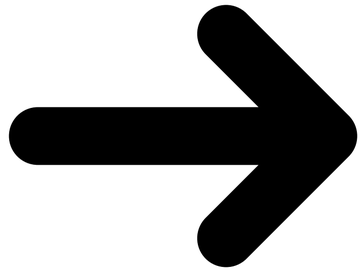
PRG PRF



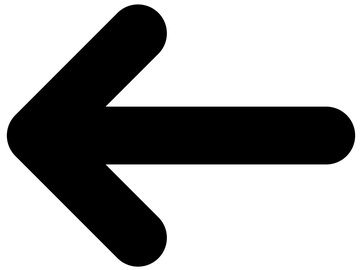
Given a PRG, build a PRF

Given a PRF, build a PRG

“Straightforward”, homework problem



PRG PRF



Given a PRG, build a PRF

Harder

$$f : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{n}$$

f is called a **one-way function** if for any PPT program A and for all inputs x the following probability is negligible:

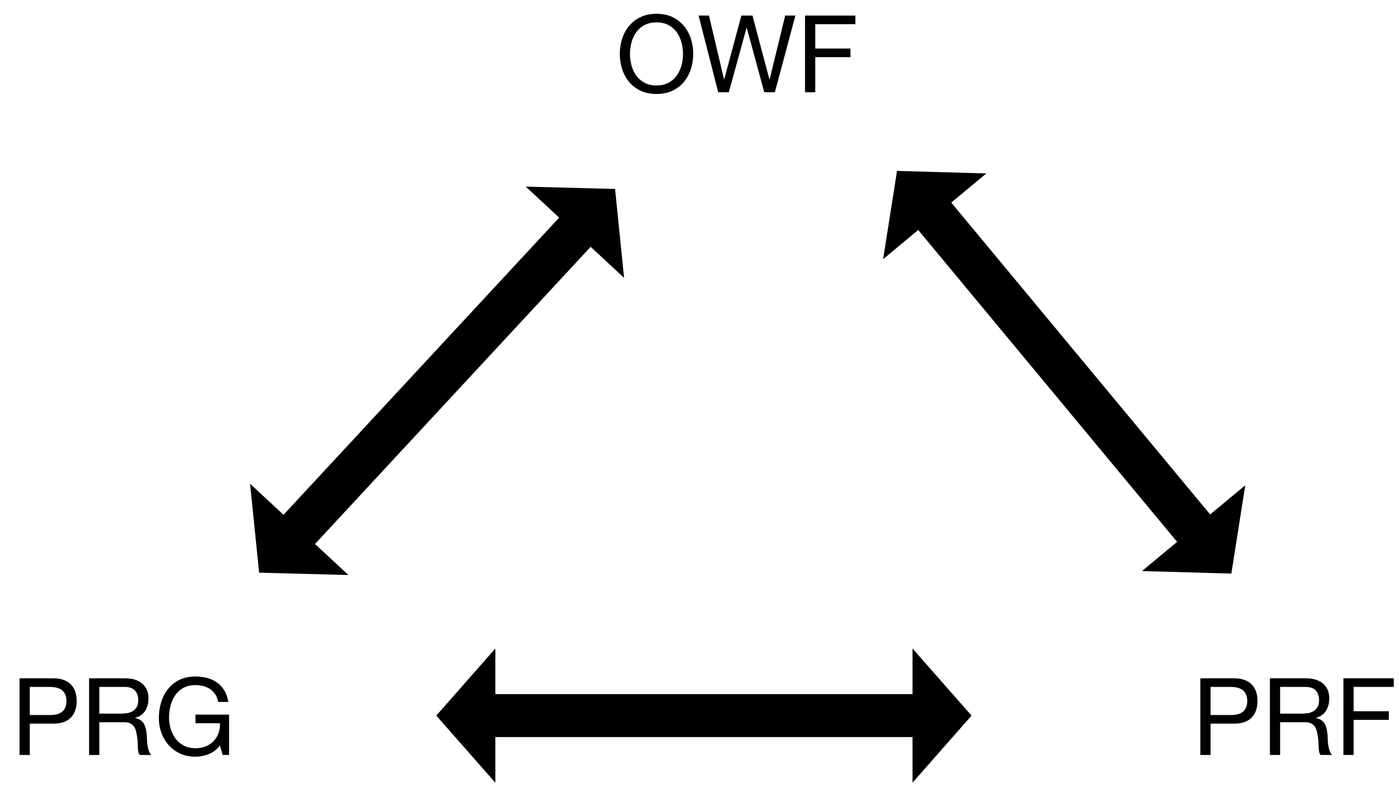
$$\Pr\left[f(A(f(x)) = f(x) \;\middle|\; x \leftarrow \{0,1\}^{\lambda} \right]$$

$$f : \{0,1\}^{\lambda} \rightarrow \{0,1\}^{n}$$

f is called a **one-way function** if for any PPT program A and for all inputs x the following probability is negligible:

$$\Pr\left[f(A(f(x)) = f(x) \;\middle|\; x \leftarrow \{0,1\}^{\lambda} \right]$$

"f is hard to invert"



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

Modern Cryptography

State assumptions **PRGs exist**

Define security

Design system

Prove: if assumption holds, system meets definition

Modern Cryptography

State assumptions

Define security

Design system

Prove: if assumption holds, system meets definition

Today’s objectives

Use PRG to define a new cipher

Define one-time secure cipher

Prove our cipher satisfies one-time security

Introduce Pseudorandom Functions (PRFs) and one-way functions

Discuss connections between PRGs, PRFs, OWFs