

CSCI 1515 Applied Cryptography

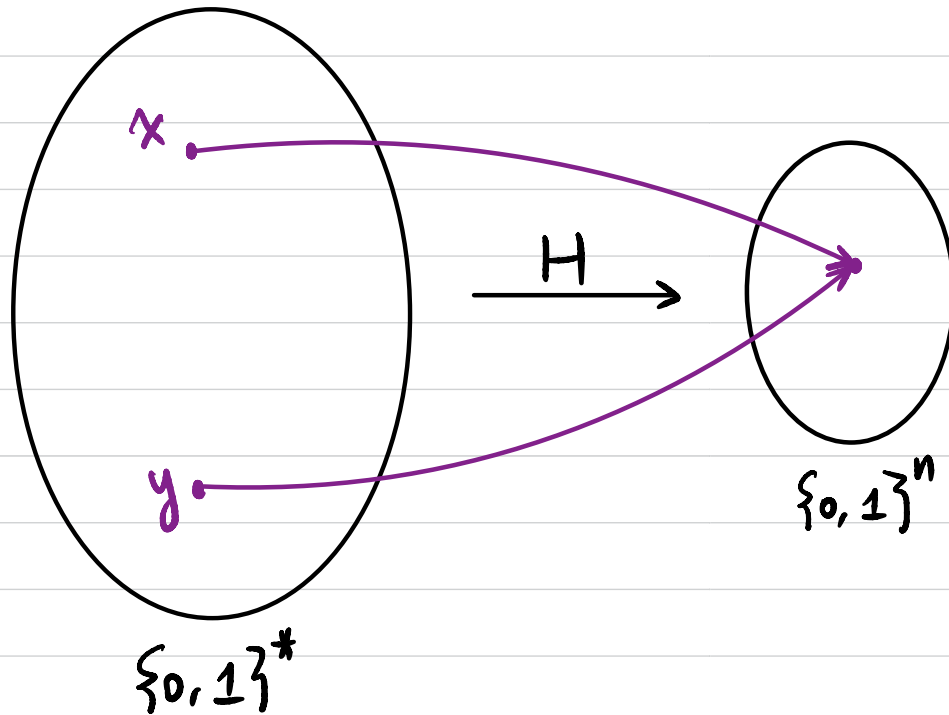
This Lecture:

- Cryptographic Hash Functions (Continued)
- Putting it All Together: Secure Communication
- Pseudorandom Generator (PRG)
Pseudorandom Function (PRF)
Pseudorandom Permutation (PRP)

Hash Function

$$H: \{0,1\}^* \rightarrow \{0,1\}^n \quad \theta(\lambda)$$

$$\lambda = 128$$
$$n = 256$$



Collision-Resistant Hash Function (CRHF):

It's computationally hard to find $x, y \in \{0,1\}^*$ s.t.

$$x \neq y, \quad H(x) = H(y) \quad (\text{collision})$$

Birthday Problem / Paradox

There are q students in a class.

Assume each student's birthday is a random $y_i \in [365]$

What's the probability of a collision?

$$q = 366 \Rightarrow \text{prob.} = 1$$

$$q = 23 \Rightarrow \text{prob.} \approx 50\%$$

$$q = 70 \Rightarrow \text{prob.} \approx 99.9\%$$

$$y_i \in [N]$$

$N = 2^n$

$$q = N + 1 \Rightarrow \text{prob.} = 1$$

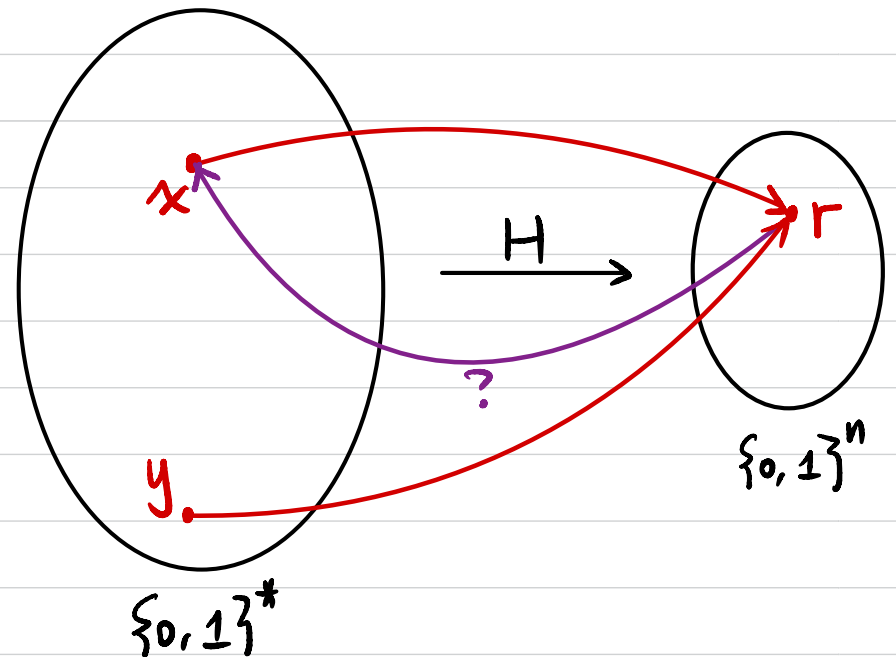
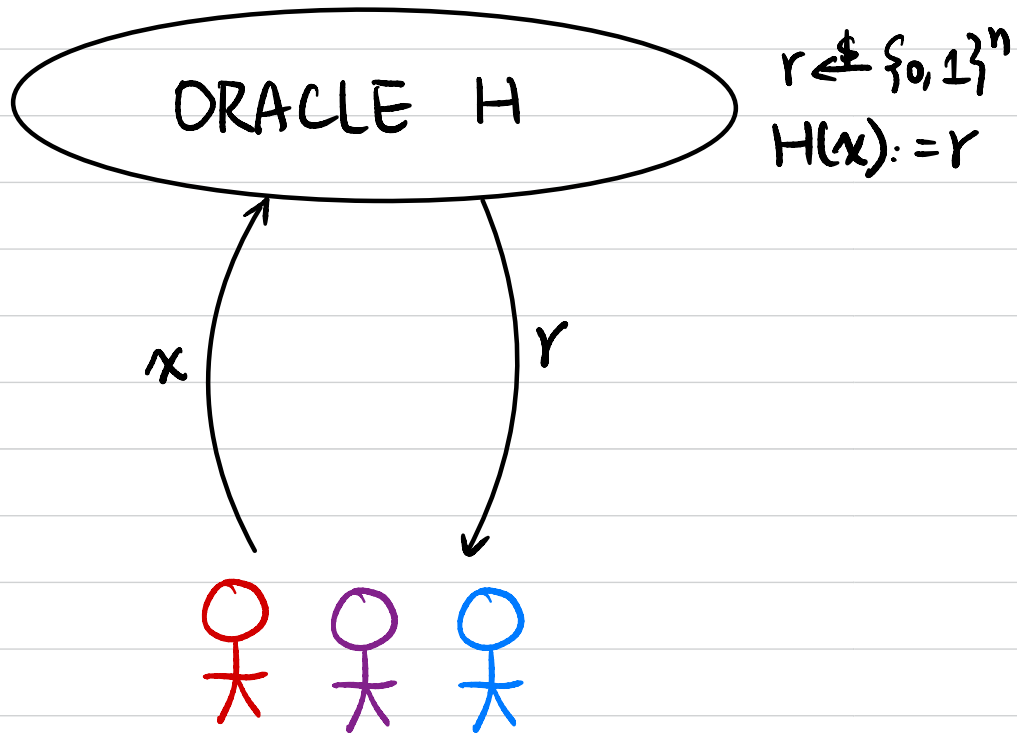
$$q = \sqrt{N} \Rightarrow \text{prob.} \approx 50\%$$

$$q \sim 2^{128}$$

$$2^{128} \sim \sqrt{2^n} \Rightarrow n = 256$$

Random Oracle Model

$$H: \{0,1\}^* \rightarrow \{0,1\}^n$$



Constructions for Hash Function

MD5: output length 128-bit
best known attack 2^{16}
Collision found in 2004

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-0: Standardized in 1993
output length 160-bit
best known attack 2^{39}
- SHA-1: Standardized in 1995
output length 160-bit
best known attack 2^{63}
Collision found in 2017

Constructions for Hash Function

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-2: Standardized in 2001
output length 224, 256, 384, 512-bit
- SHA-3: Competition 2007-2012
released in 2015
output length 224, 256, 384, 512-bit

Applications of Hash Functions

- **HMAC**

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

$$\text{Mac}_k(m) = H(k \parallel m)$$

$$\text{HMAC}_k(m) = H(\underbrace{k_2}_{k \oplus \text{opad}} \parallel \underbrace{H(\underbrace{k_1}_{k \oplus \text{ipad}} \parallel m)})$$

public

- **Hash-and-Sign** : $\text{Sign}_{sk}(H(m))$

RSA Signature : $\text{Sign}_{sk}(m) = H(m)^d \bmod N$

- **Password-based Authentication**

username, $H(\text{password})$

Applications of Hash Functions

- Deduplication

$$\begin{aligned} H(D_1) &\rightarrow h_1 \\ H(D_2) &\rightarrow h_2 \end{aligned}$$

← unique identifier

$$\text{If } h_1 \neq h_2 \Rightarrow D_1 \neq D_2$$

$$\text{If } h_1 = h_2 \Rightarrow D_1 = D_2 \text{ (why?)}$$

Virus Scan

$$H(F) \stackrel{?}{=} H(F^*)$$

Video Deduplication

$$H(V_1) \stackrel{?}{=} H(V_2)$$

Applications of Hash Functions

- HKDF (Key Derivation Function):

$$\text{HMAC}(g^{ab}, \text{salt})$$

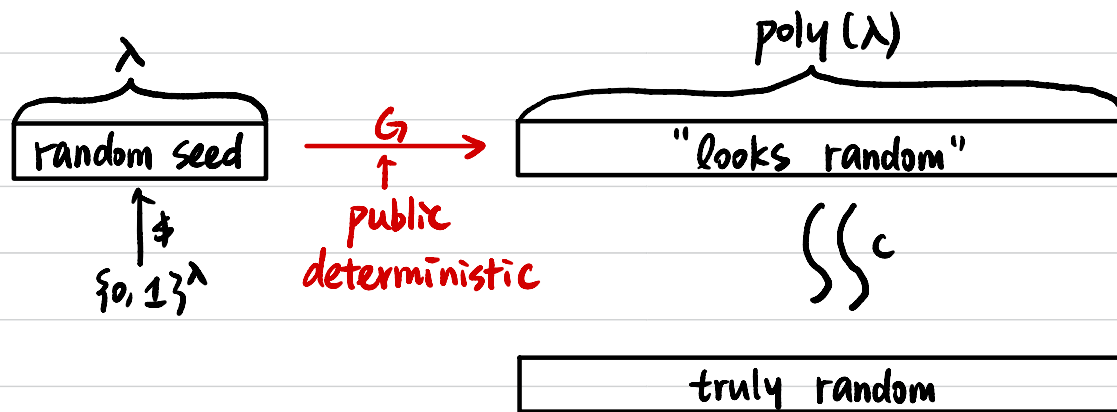
$$H(g^{ab} || 0 \dots 0)$$

$$H(g^{ab} || 0 \dots 1)$$

$$H(g^{ab} || 0 \dots 10)$$

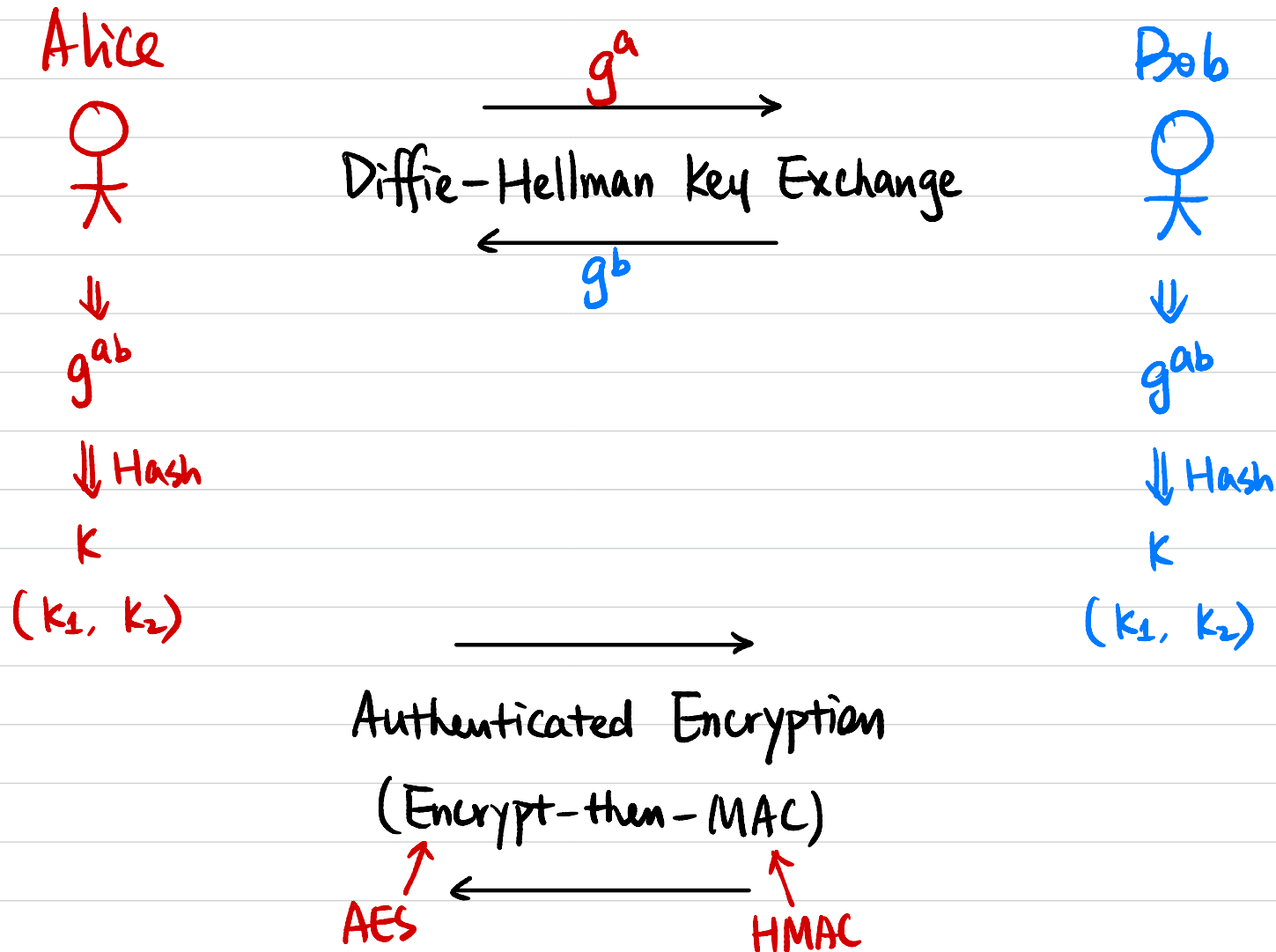
⋮

Pseudorandom Generator (PRG)



- Fast Membership Proof (Merkle Tree)
 - Blockchain
 - Key Transparency

Putting it All Together: Secure Communication



Any security issue?

Signal: Diffie-Hellman Ratchet

Alice



$\Downarrow a_1$

$g^{a_1 b_1}$

$\Downarrow$

k_1

$\Downarrow a_2$

$g^{a_2 b_1}$

$\Downarrow$

k_2

$\Downarrow a_3$

$g^{a_3 b_2}$

$\Downarrow$

k_3

Diffie-Hellman Key Exchange

g^{a_1}

g^{b_1}

g^{a_2}

g^{b_2}

Bob



$\Downarrow b_1$

$g^{a_1 b_1}$

$\Downarrow$

k_1

$\Downarrow b_2$

$g^{a_2 b_1}$

$\Downarrow$

k_2

$\Downarrow b_3$

$g^{a_3 b_2}$

$\Downarrow$

k_3

If k_1 is leaked?

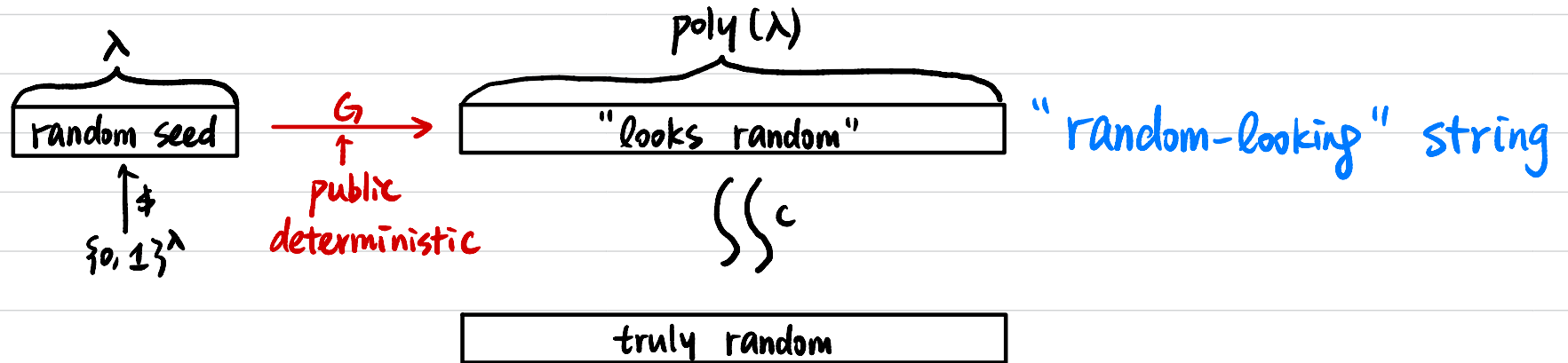
If b_1 is leaked?

Summary

	Symmetric-Key	Public-Key
Message Secrecy	Primitive: SKE Construction: block cipher	Primitive: PKE Constructions: RSA / ElGamal
Message Integrity	Primitive: MAC Constructions: CBC-MAC / HMAC	Primitive: Signature Constructions: RSA / DSA
Secrecy & Integrity	Primitive: AE Construction: Encrypt-then-MAC	
Key Exchange		Construction: Diffie-Hellman
Important Tool	Primitive: Hash function Construction: SHA	

Pseudorandom Function (PRF)

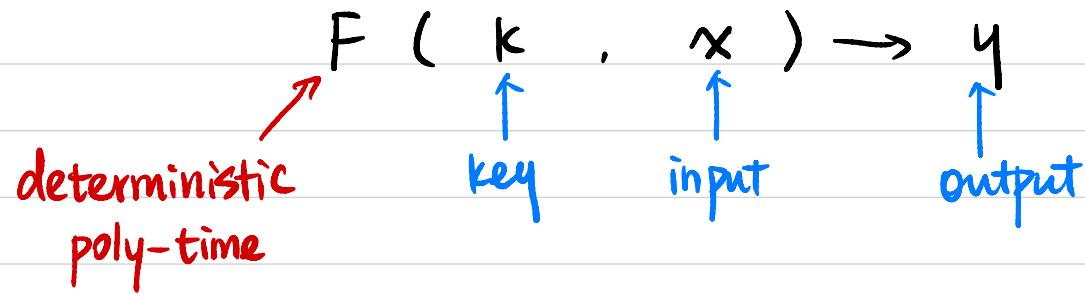
Pseudorandom Generator (PRG)



Pseudorandom Function (PRF): "random-looking" function

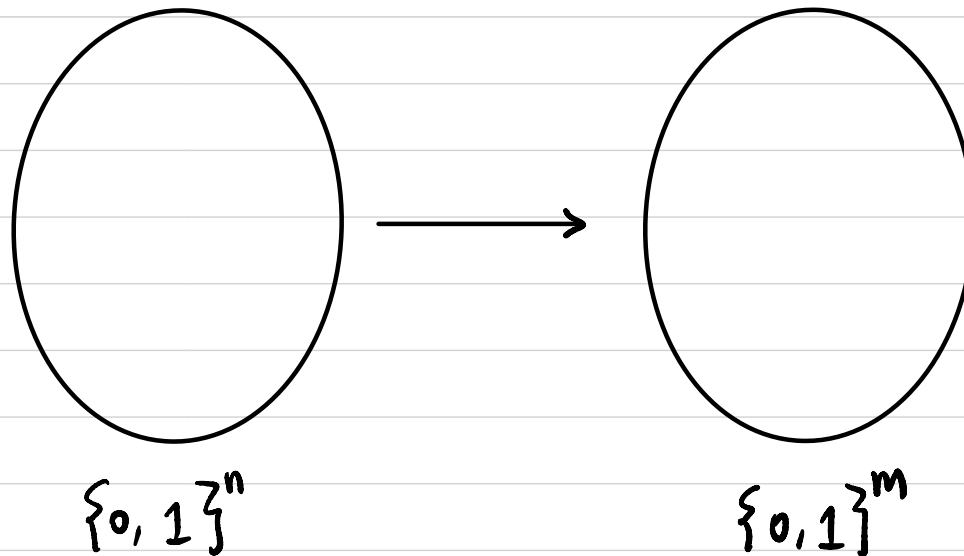
Pseudorandom Function (PRF)

Keyed Function $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^m$



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

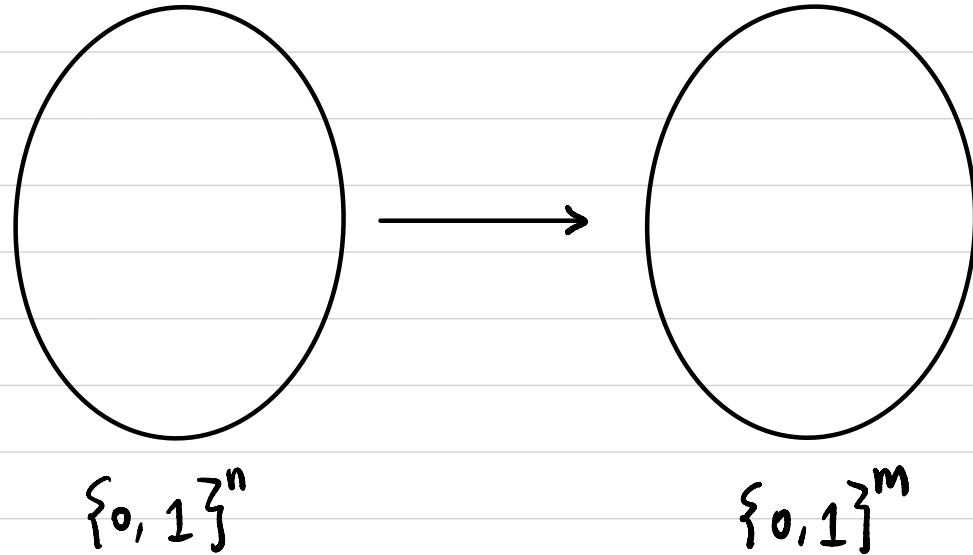
$F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

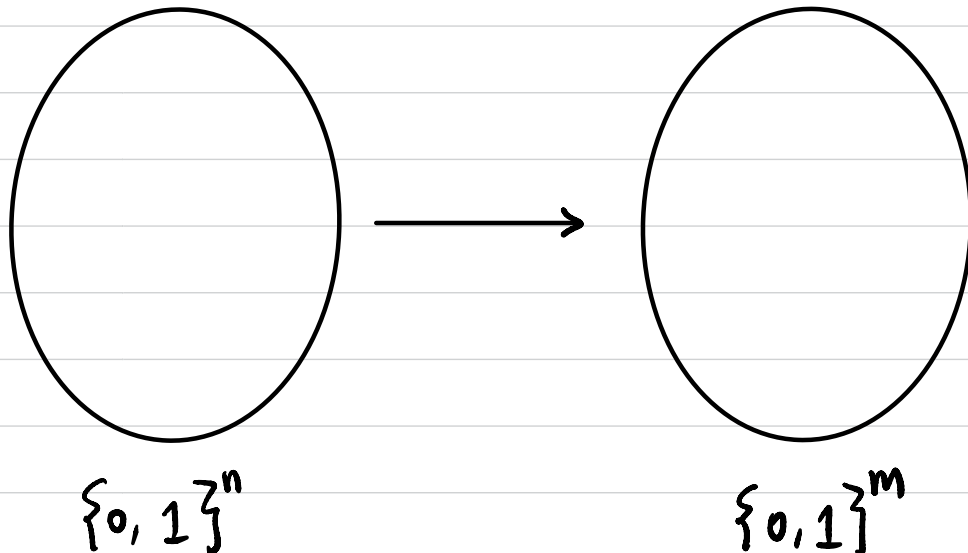
$$k \leftarrow \{0, 1\}^\lambda \quad F_k:$$



How many possible F_k 's?

$$f \leftarrow \{ F \mid F: \{0, 1\}^n \rightarrow \{0, 1\}^m \}$$

$f:$

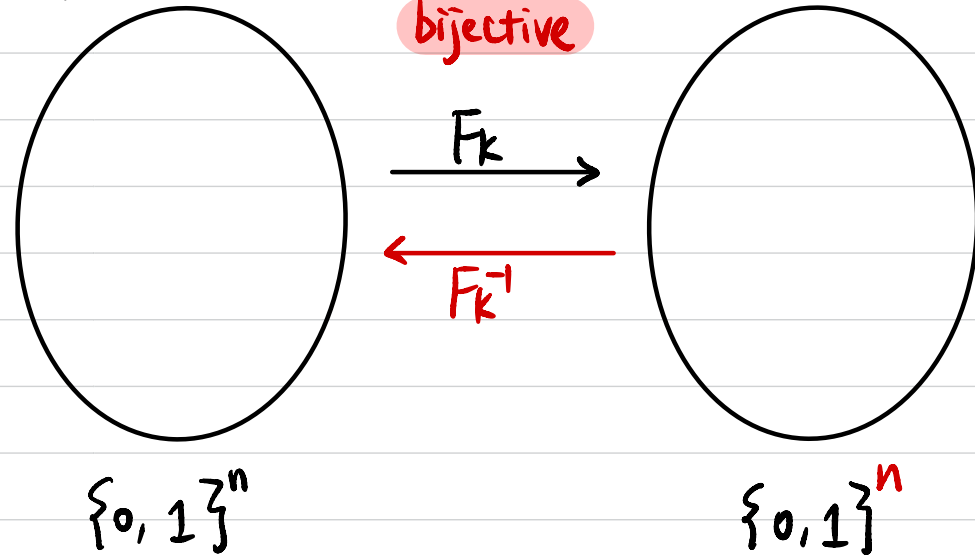


$\sum \sum^c$ (not knowing k)

How many possible f 's?

Pseudorandom Permutation (PRP)

$$k \leftarrow \{0, 1\}^{\lambda} \quad F_k:$$

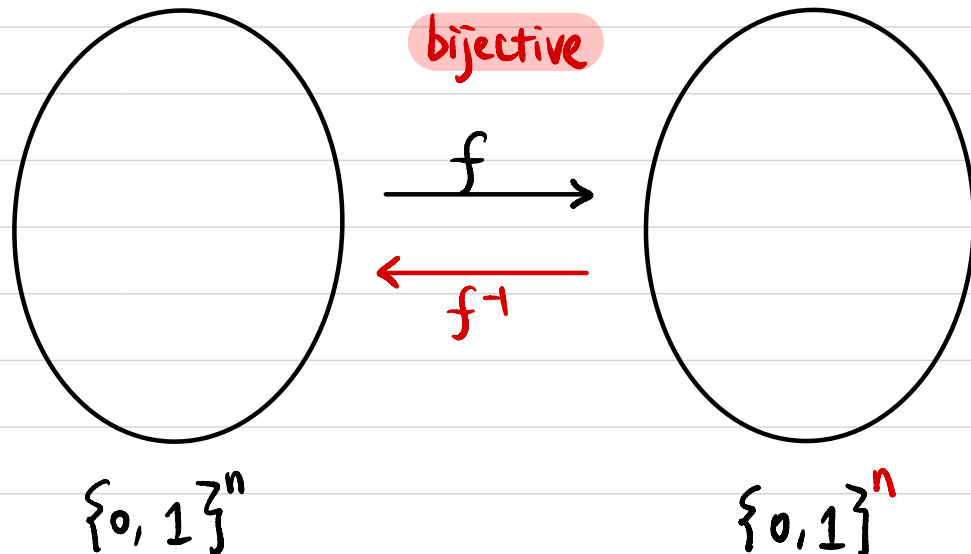


How many possible F_k 's ?

$$f \leftarrow \{ F \mid F: \{0, 1\}^n \rightarrow \{0, 1\}^n, \\ F \text{ is bijective} \}$$

$f:$

$\sum \sum^c$ (not knowing k)



How many possible f 's ?