CSCI 1515 Applied Cryptography

This Lecture:

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

Summary

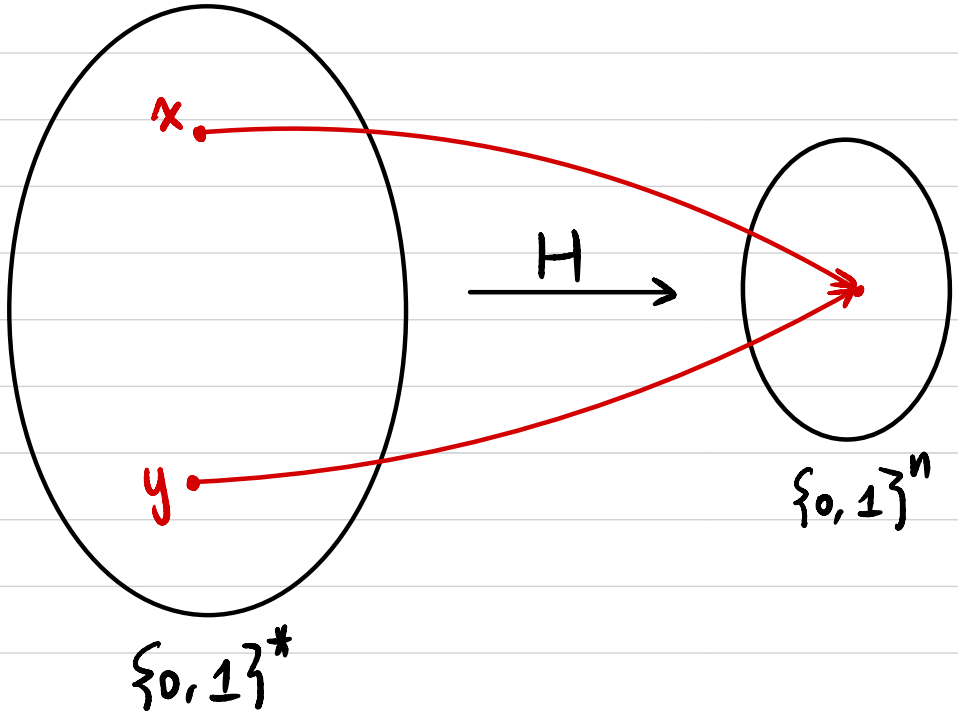
	Symmetric-Key	Public-Key
Message Secrecy	Primitive: SKE Construction: block Cipher	Primitive: PKE Constructions: RSA / ElGamal
Message Integrity	Primitive: MAC Constructions: CBC-MAC / HMAC	Primitive: Signature Constructions: RSA / DSA
Secrecy & Integrity	Primitive: AE Construction: Encrypt-then-MAC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

Hash Function

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

$\lambda = 128$

$n = 256$



Collision-Resistant Hash Function (CRHF):

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

$x \neq y$, $H(x) = H(y)$ (collision)

Birthday Problem / Paradox

There are q students in a class.

Assume each student's birthday is a random $y_i \xleftarrow{\$} [365]$

What's the probability of a collision?

$q = 366 \Rightarrow$ prob. $= 1$

$q = 23 \Rightarrow$ prob. $\simeq 50\%$

$q = 70 \Rightarrow$ prob. $\simeq 99.9\%$

$y_i \xleftarrow{\$} [N]$ ($N = 2^n$)

$q = N + 1 \Rightarrow$ prob. $= 1$

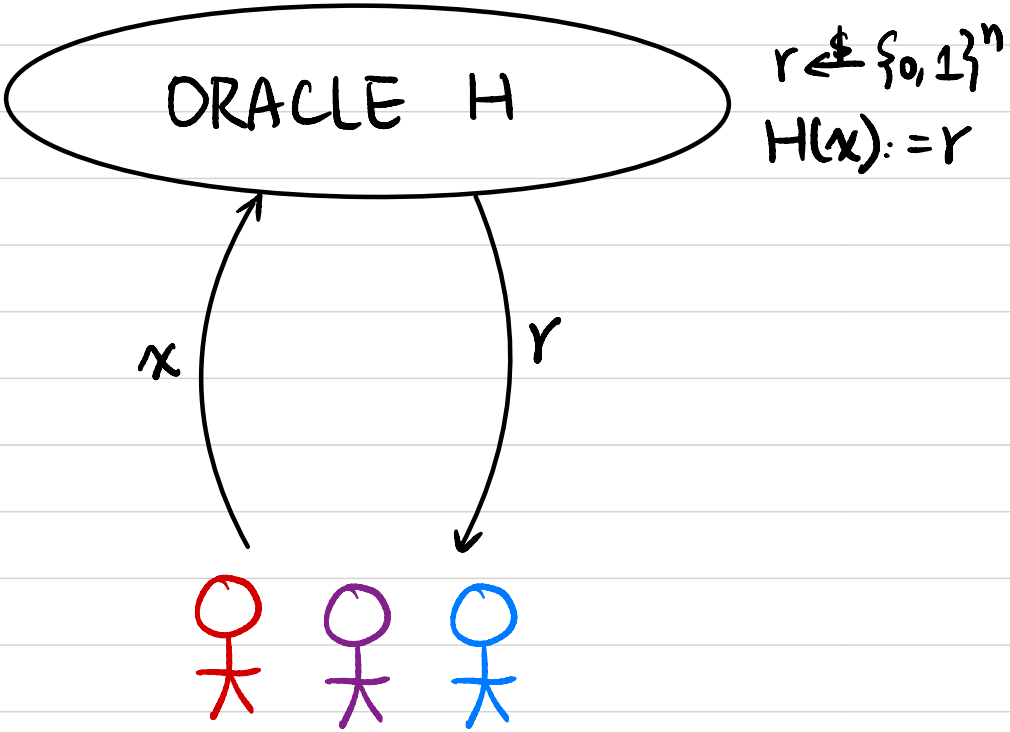
$q = \sqrt{N} \Rightarrow$ prob. $\simeq 50\%$

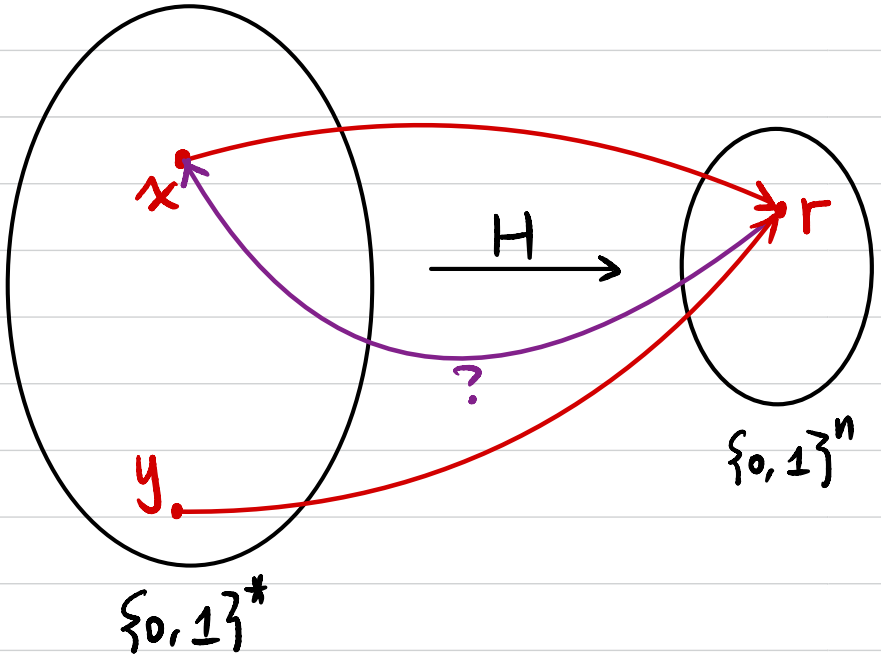
$q = 2^{128}$

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

Random Oracle Model

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





Applications of Hash Functions

- **Deduplication**

$H(D_1) \rightarrow h_1$

$H(D_2) \rightarrow h_2$

h_1, h_2: unique identifier

If $h_1 \neq h_2 \Rightarrow D_1 \neq D_2$

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

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

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

Applications of Hash Functions

- **HMAC**

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

$Mac_k(m) = H(k \| m)$

$HMAC_k(m) = H(k_1 \| H(k_2 \| m))$

$k_1 = k \oplus opad$, $k_2 = k \oplus ipad$

public

$Mac_k(m) \to t$

$Vrfy_k(m,t) \to 0/1$

Hard to forge (m^*, t^*) where $t^* = H(k \| m^*)$

- **Hash-and-Sign**: $Sign_{sk}(H(m))$

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

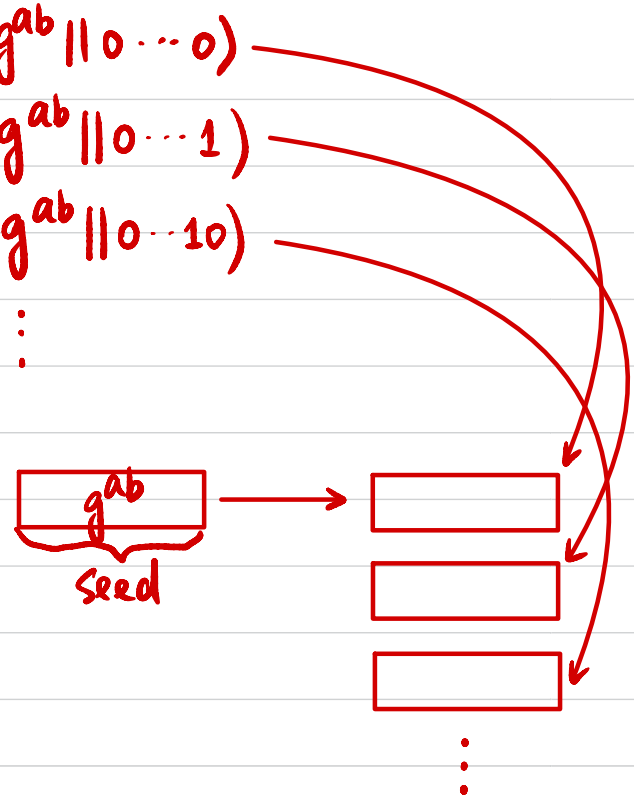
- **Password-based Authentication**

username, H(password)

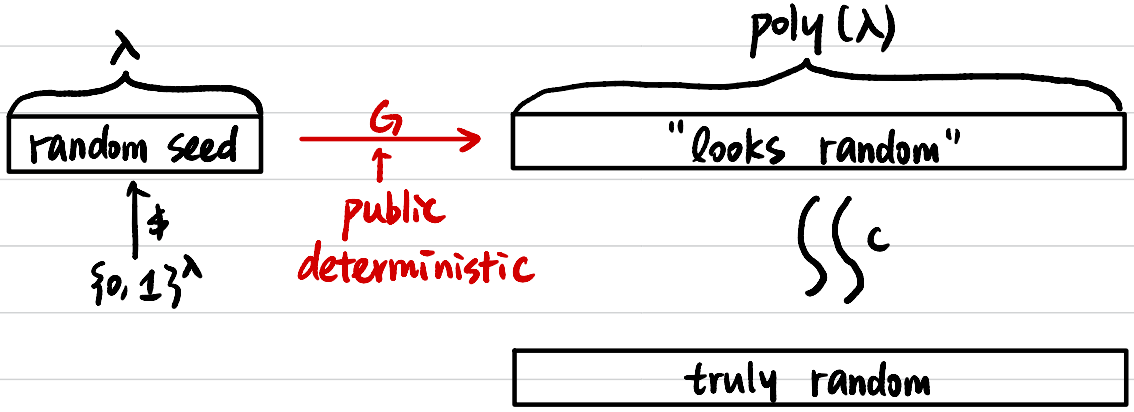
Applications of Hash Functions

- **HKDF (Key Derivation Function):**

  $HMAC(g^{ab} \| salt)$

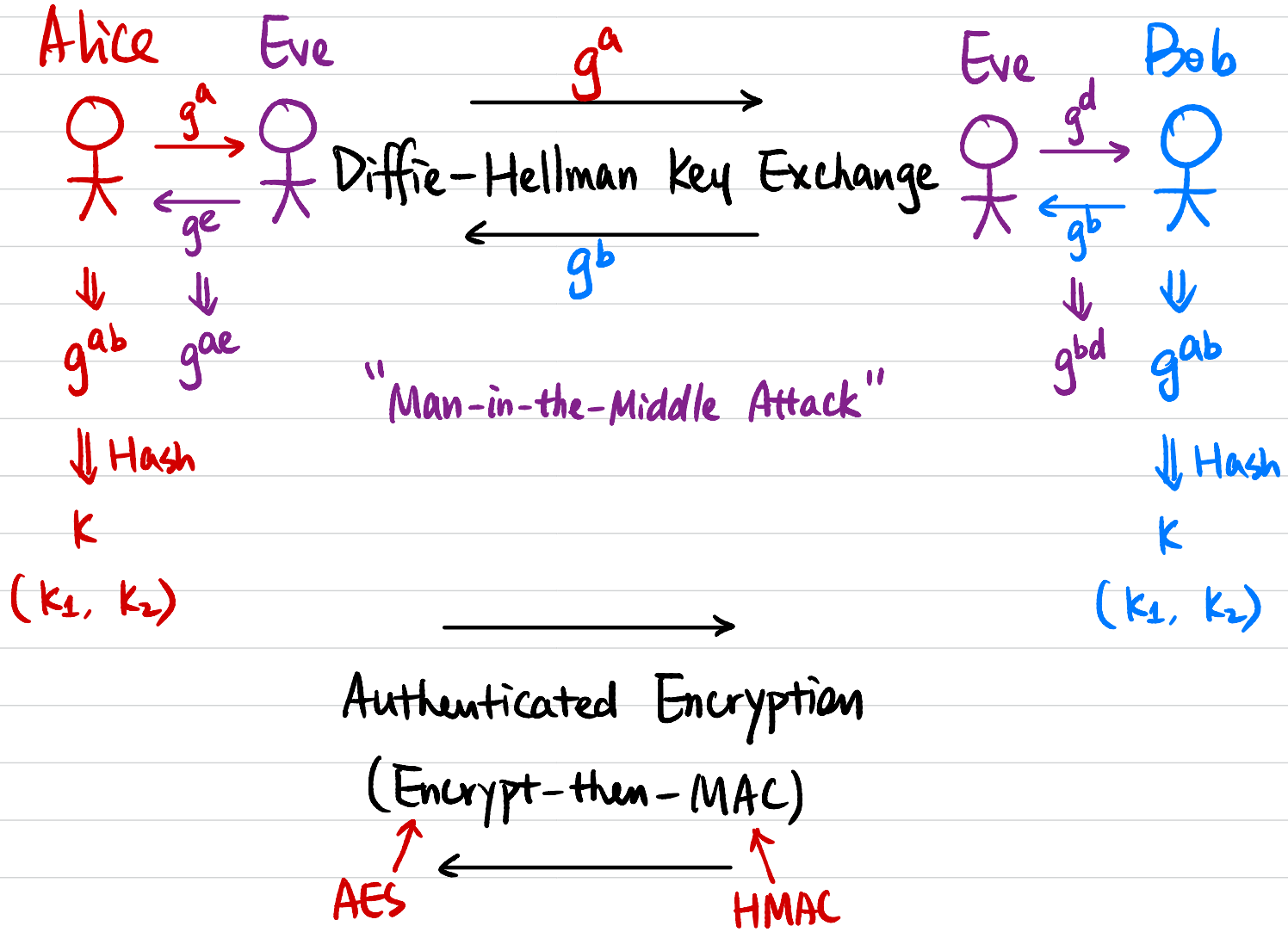


Pseudorandom Generator (PRG)



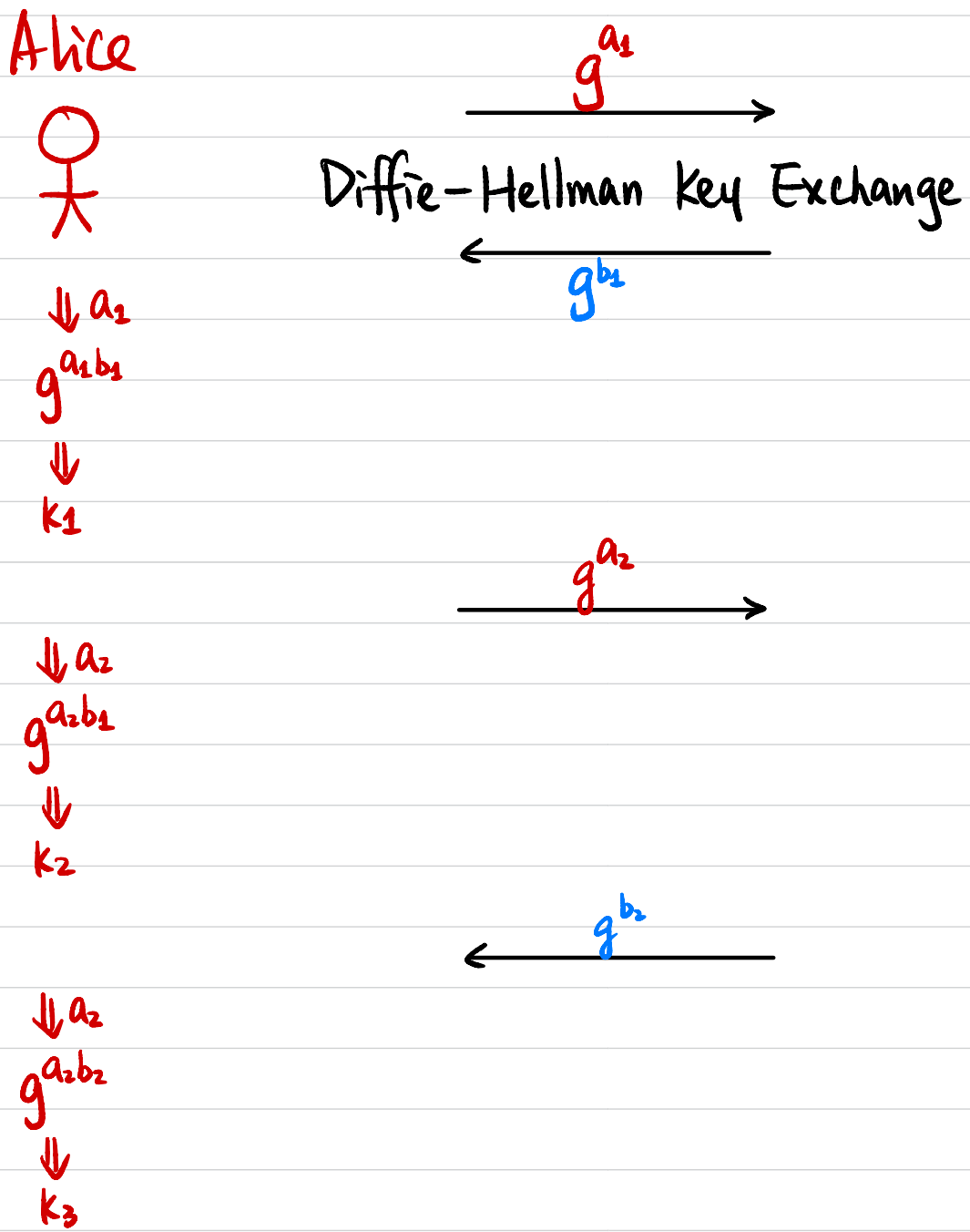
- Fast Membership Proof (**Merkle Tree**)
  - Blockchain
  - Key Transparency

Putting it All Together: Secure Communication



Any security issues?

Signal: Diffie-Hellman Ratchet



Adv. sees:

g^{a_1} g^{b_1} g^{a_2} g^{b_2}

If b_1 is leaked?

$(g^{a_1})^{b_1} \rightarrow g^{a_1 b_1} \rightarrow k_1$

$(g^{a_2})^{b_1} \rightarrow g^{a_2 b_1} \rightarrow k_2$

If k_1 is leaked?

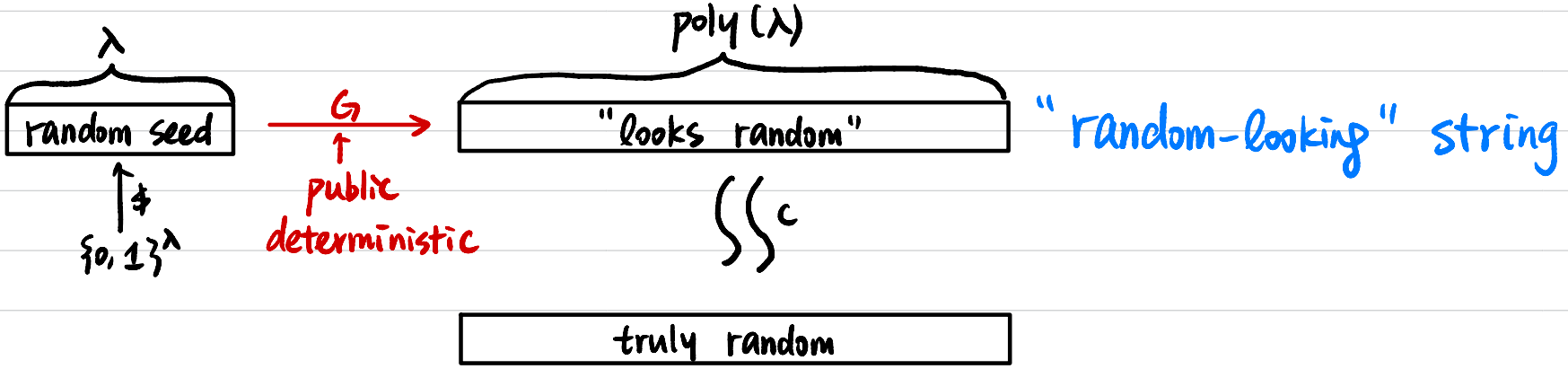
Only k_1

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

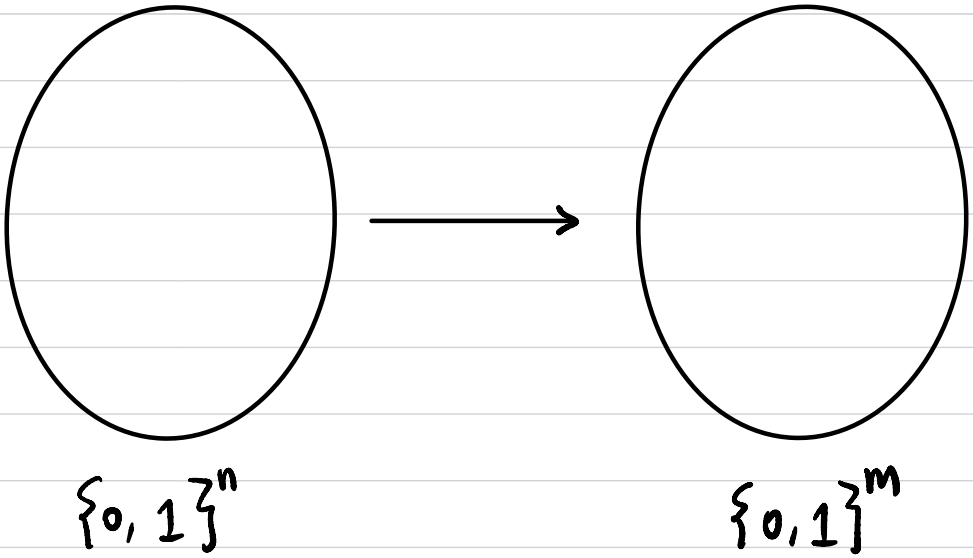
Pseudorandom Function (PRF)

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

$F(k, x) \to y$

- F: deterministic poly-time
- k: key
- x: input
- y: output

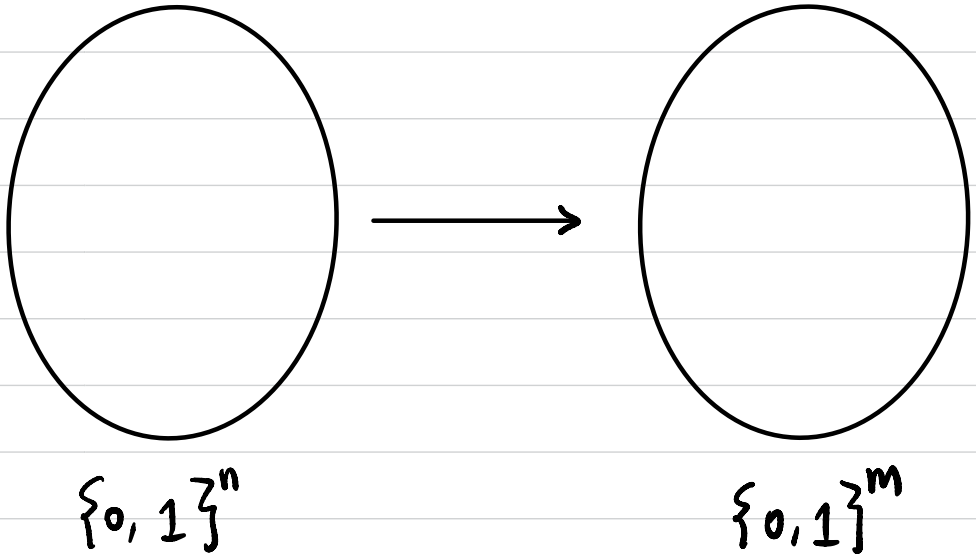
$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

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



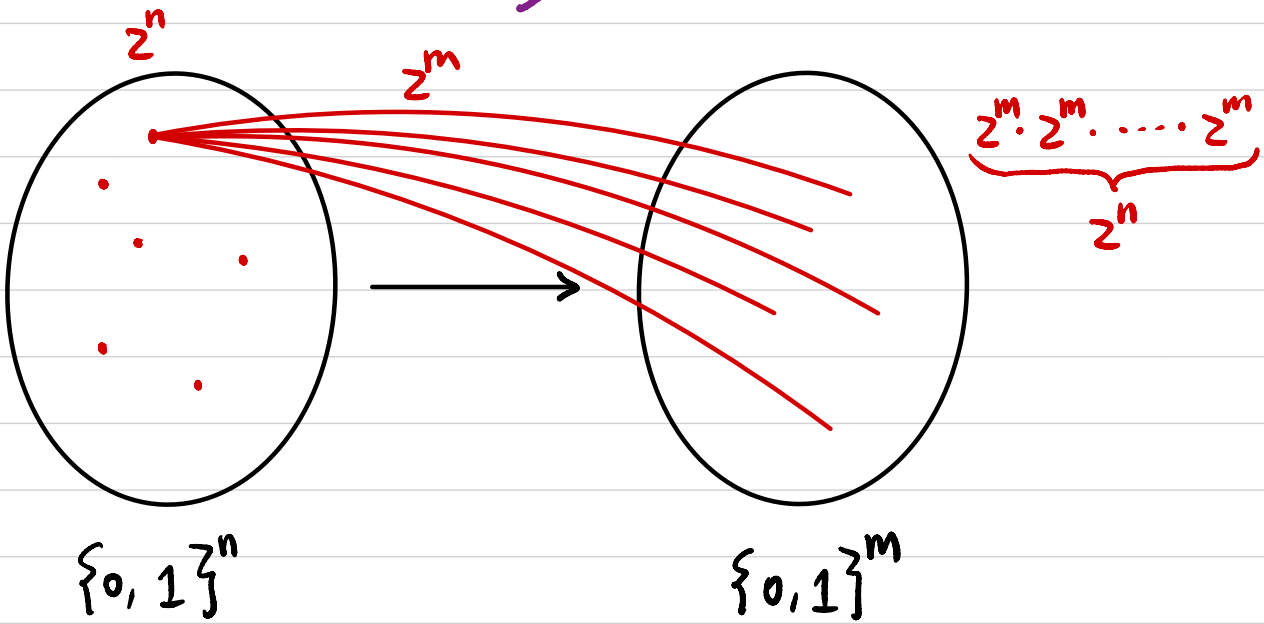
How many possible F_k's ?

2^λ

$\approx\approx c$ (not knowing k)

$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^m \}$

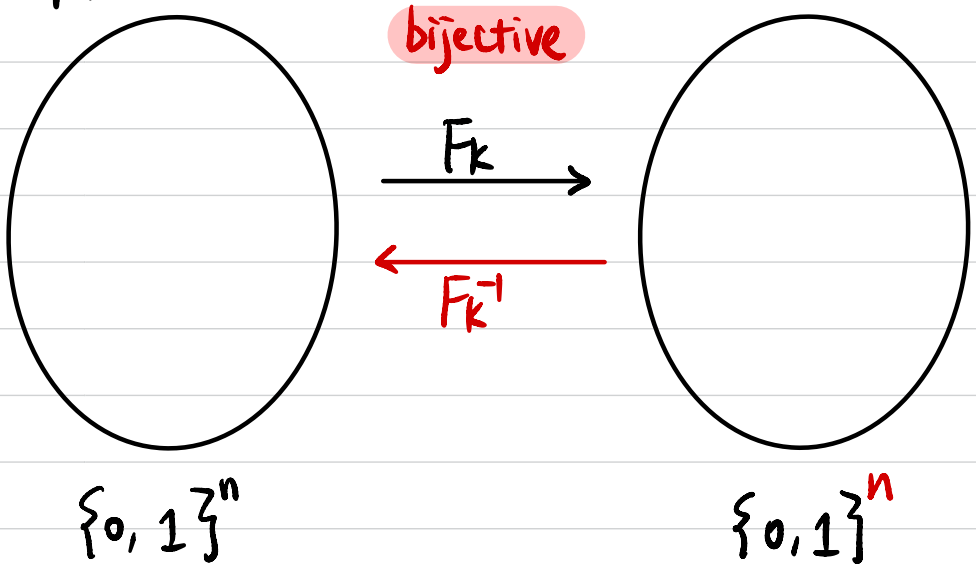
$(2^m)^{2^n} = 2^{m \cdot 2^n}$ $\quad f:$



How many possible f's ?

Pseudorandom Permutation (PRP)

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



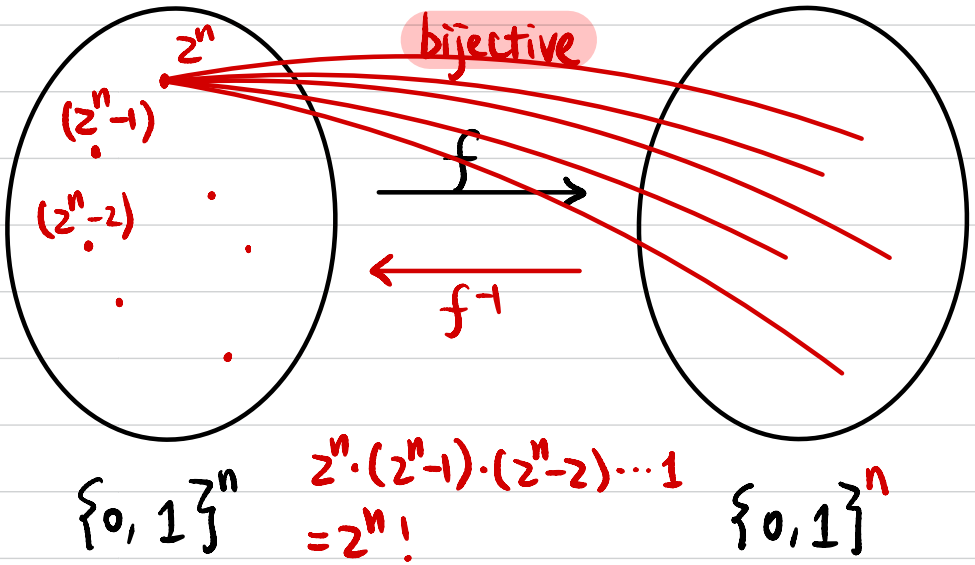
How many possible F_k's ?

2^λ

$\{\{\}\}_c$ (not knowing k)

$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^n,$ F is bijective $\}$

$2^n!$ $\quad f:$



How many possible f's ?

Constructions for Hash Function

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

Secure Hash Functions (SHA): Standardized by NIST.

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