ASYMMETRIC KEY ENCRYPTION

PK_A, SK_A

SCHEMA

KEYGEN() → (PK, SK)

ENC(PK, m) → c

DEC(SK, c) → m

PK_B, SK_B

ONE-WAY FUNCTIONS

Given x, it is easy to compute $f(x)$

Given y, it is hard to find any x s.t. $f(x) = y$

$f(x) = x$	NO	(easy to invert)
$f(x) = 1$	NO	(any x leads to 1)
$f(x) = E_K(x)$	YES	(indinguishable from random permutation)

DISCRETE LOGARITHM PROBLEM ← A very famous one-way function!

$f(x) = g^x \bmod p$ p = large prime g = random value $[2, p-1]$

This is a one-way function!

- Easy to compute (use repeated squaring)
- Hard to invert (due to log cycles)

DIFFIE-HELLMAN KEY EXCHANGE

Public Values

Large Prime, p

Random Value, g $1 < g < p-1$

$a \leftarrow$ RANDOM$(1, p-2)$

$A = g^a \bmod p$

PRIVATE KEYS

PUBLIC KEYS

$b \leftarrow$ RANDOM$(1, p-2)$

$B = g^b \bmod p$

$K = A^B = g^{ab} \bmod p$

SYMMETRIC KEY

K

$K = B^A = g^{ab} \bmod p$

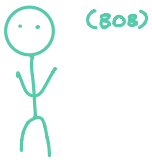
EL GAMAL ENCRYPTION

Public Values

Large Prime, p

Random Value, g $\quad 1 < g < p-1$

ALICE WANTS TO SEND A MESSAGE TO BOB.



SECRET → $K \leftarrow$ RANDOM $(1, p-2)$

PUBLIC ← $PK = g^K \bmod p$

ENC(PK, m):

- Pick a random $r \in [1, p-1]$
- $C = (g^r \bmod p \; ; \; m \cdot PK^r \bmod p)$

C_1 $\quad$ C_2

DEC$(SK, (C_1, C_2))$:

$$\frac{C_2}{C_1^K} = \frac{m \cdot (g^K \bmod p)^r}{(g^r \bmod p)^K} = m$$

CRYPTOGRAPHIC HASH FUNCTIONS

One-way + Collision Resistant

One-Way: intuitively, we can't decipher the original value given a hash

Collision-Resistant: no two things hash to the same value

$H(x) = x$	Collision Resistant
$H(x) = 3$	None
$H(x) = SHA256(x)$	Both

Why isn't $H(x) = 3$ one-way?

Referring to the definition of one-way...

Given y, easy to find x s.t. $H(x) = y$