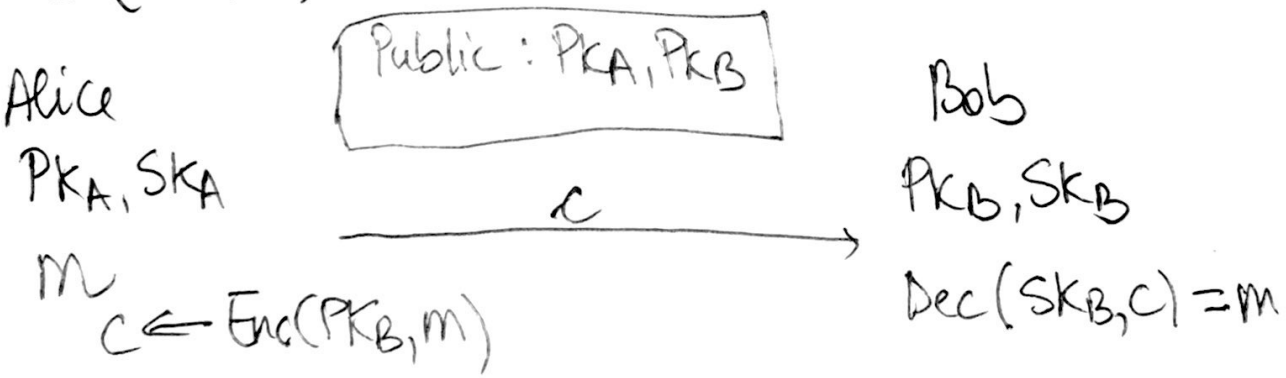
Last time: Diffie Hellman key exchange

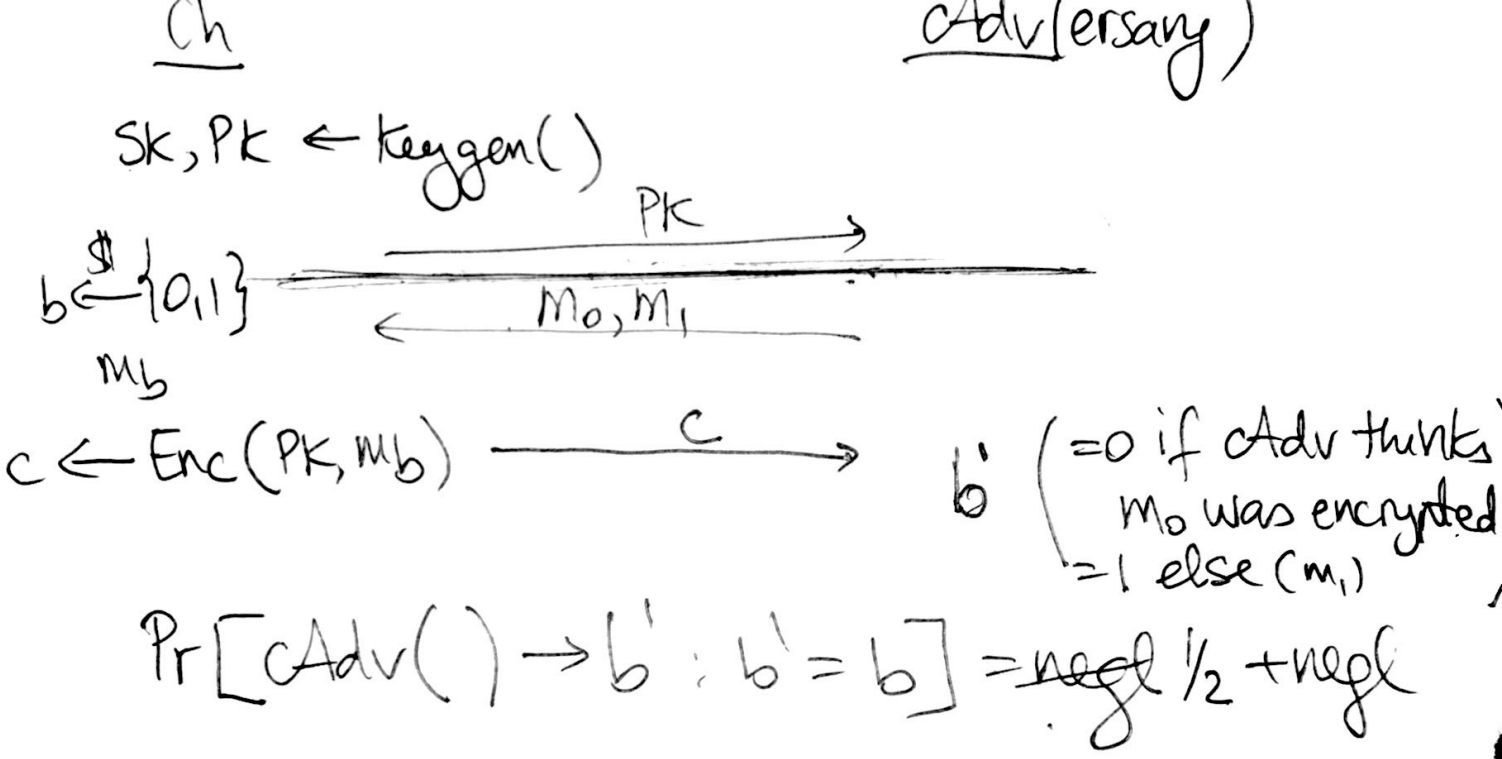
Public-key encryption

KeyGen( ) → SK, PK
Enc(PK, m) → c
Dec (SK, c) → m

⇒ asymmetric cryptography



Security: (Similar to IND-CPA) called semantic security



$$Pr[cAdv() \to b' : b' = b] = \text{negl}\ 1/2 + \text{negl}$$

El Gamal encryption (1985)

KeyGen():
- generate random prime p (large, 2048-bits),
  - g $1 < g < p-1$
  - k $0 < k < p-1$

$SK = k$; $PK = g^k \bmod p$; p, g

secret — public

Safe because of Discrete Log Assumption & Diffie-Hellman Decision Assumption

$Enc(PK, m)$: $m \in [1, p-1]$

- pick random $r \in [1, p-1]$ (secret)

NO r in C!!!

$C = [g^r \bmod p ;\ m \cdot PK^r \bmod p]$

k → (C_1, C_2)

$Dec(SK, C)$:

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

does not hide a message that is 0

$m \neq 0$

Alice knows PK_B

Bob

SK_B

Strawman

$Enc(PK_B, P_1)$; $Enc(PK_B, P_2)$ . . . $Enc(PK_B, P_n)$ } n public key encr.

Slow

big files Better:

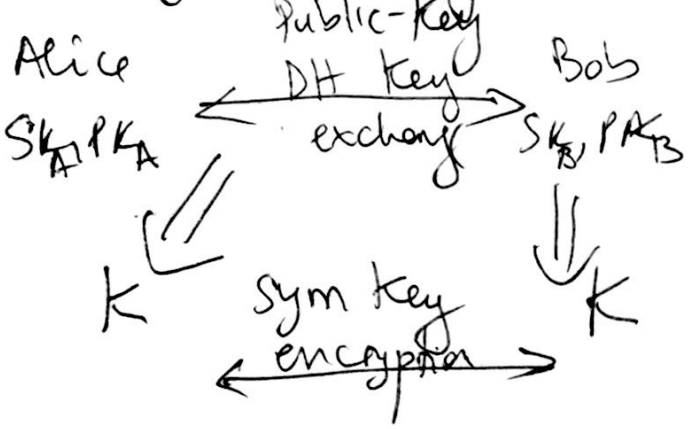
→ Alice generates symmetric key K

Enc(K, file) [CTR mode . . .] : symmetric-key enc.

Enc (PK_B, K) : public key enc → only one PK enc

sym. key enc >> faster PK enc

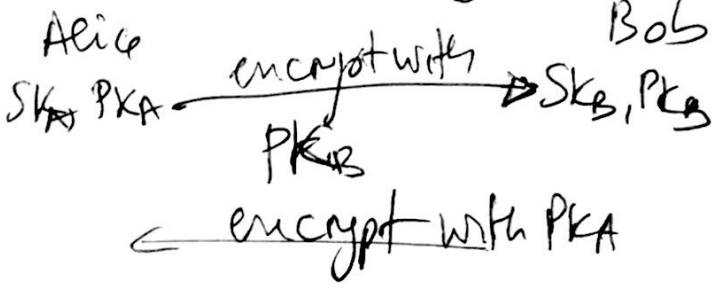
DH key exchange



interactive

SSL encrypted communications when parties are online

PK Encryption



non-interactive

e.g. email, when a party is offline

Cryptographic hash functions

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

any size — fixed length

SHA256 ⇒ 256 bits of output

$H(x)$ = hash of x

digest / fingerprint of x

the output of H looks like a random string.

$x = 1\,0\,0\,1\,0\,1\,1\,\ldots\,1\,1$ | 0

$y = \_\_\_\_\_$ | 1

$H(x)$ very different, $H(y)$ roughly half bits different

deterministic

Security:

1) one-way function: ∀ poly-time attackers

$$\Pr[x \xleftarrow{\$} \{\}; y \leftarrow H(x); A(y) = x' : H(x') = y] = \text{negl}$$

2) Collision resistance

No one can find x and x' s.t. $H(x) = H(x')$, $x \neq x'$