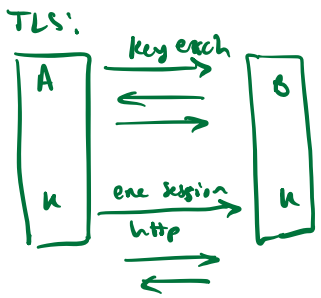
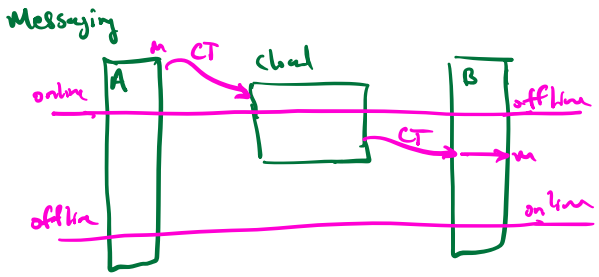
Public-Key Encryption.

Two settings for communication.

interactive

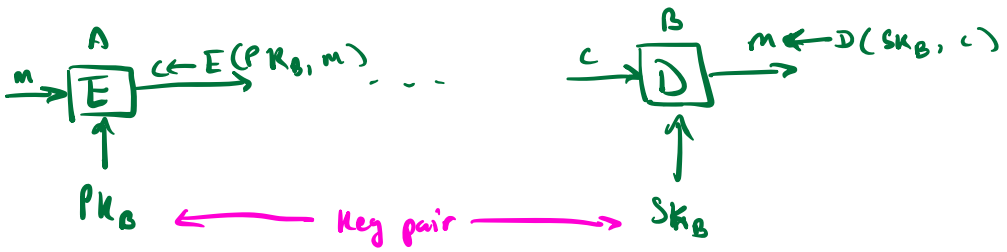


noninteractive



how??

PKE model



PK: public key

SK: secret key

Def. a PKE scheme over $(\mathcal{M}, \mathcal{C})$

is a triple of algs. (Gen, E, D) where

→ $Gen() \to (PK, SK)$ rand. alg. that outputs key pair

→ $E(PK, m) \to c$: rand. alg.

→ $D(SK, c) \to m$ or reject : det. alg

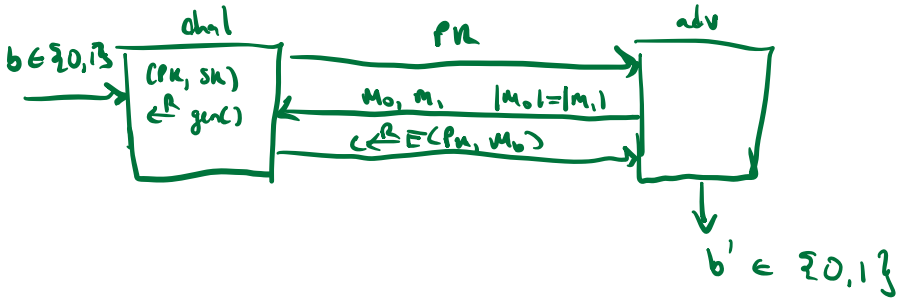
s.t. if $(PK, SK) \xleftarrow{R} Gen()$ then

$$\forall m \in \mathcal{M} \quad D(SK, E(PK, m)) = m$$

note: recipient knows nothing about ID of sender

Semantic security for PKE (security against eavesdropping)

For $b = 0, 1$ def. $EXP(0)$, $EXP(1)$ as



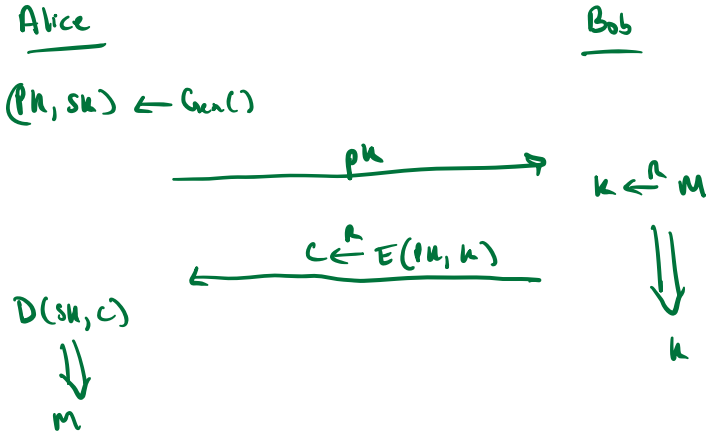
Def. $\Sigma = (Gen, E, D)$ is semsec if

$\forall$ eff. A:

$$Adv[A, \Sigma] := \left| Pr[EXP(0) = 1] - Pr[EXP(1) = 1] \right| \text{ is "negl"}$$

note: requires E to be a rand. fn.

Toy key exchange from PKE (secure against eavesdropping)



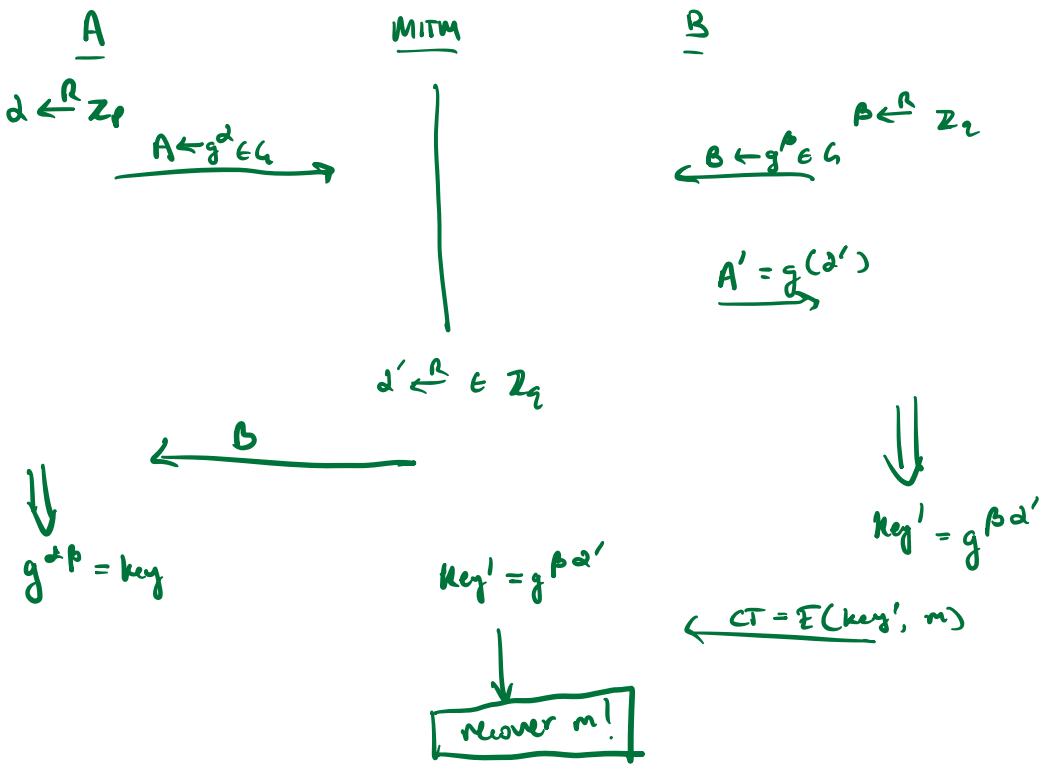
Security: eavesdropper sees PK, $E(PK, k)$ and wants k

PKE semsec $\Rightarrow$ Adv cannot distinguish $(PK, E(PK, k))$ from $(PK, E(PK, 0))$

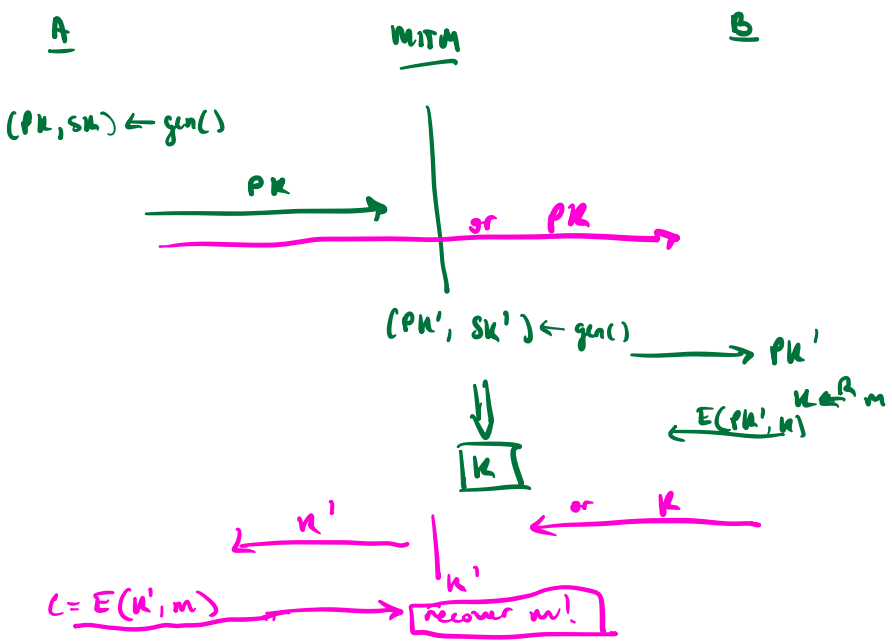
$\Rightarrow$ Adv learns nothing about k

Both toy key-exchange protocols are insecure against MITM attacks

DH attack



PKE attack



Both are toy protocols.

Need more machinery to defend against MITM

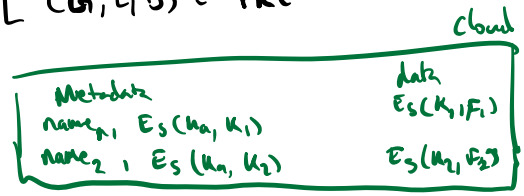
=> digital signatures.

Other PKE applications

File sharing in encrypted filesystem.

(E_s, D_s): sym. cipher over (K, M, C)

(G, E, D): PKE



Alice: $k_a \xleftarrow{R} K$

Alice uploads file F_1:

$k_1 \xleftarrow{R} K$

compute $E_s(k_1, F_1)$, $E_s(k_a, k_1)$

Alice wants to give Bob access to F_1 but not F_2

→ Get PK_B from cloud

→ Upload $E(PK_B, k_1)$ to cloud

→ Now Bob can R/W F_1

Note: no interaction between A, B