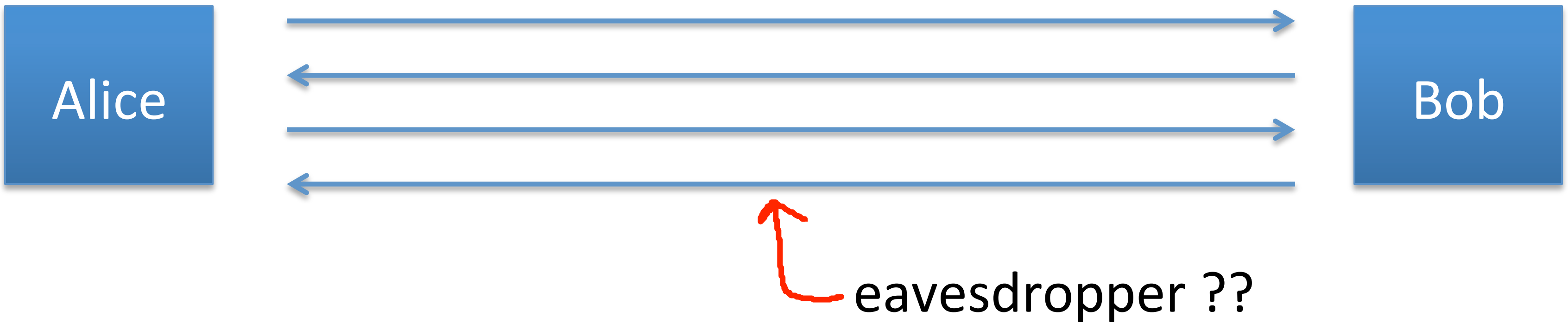
Basic key exchange

Public-key encryption

Establishing a shared secret

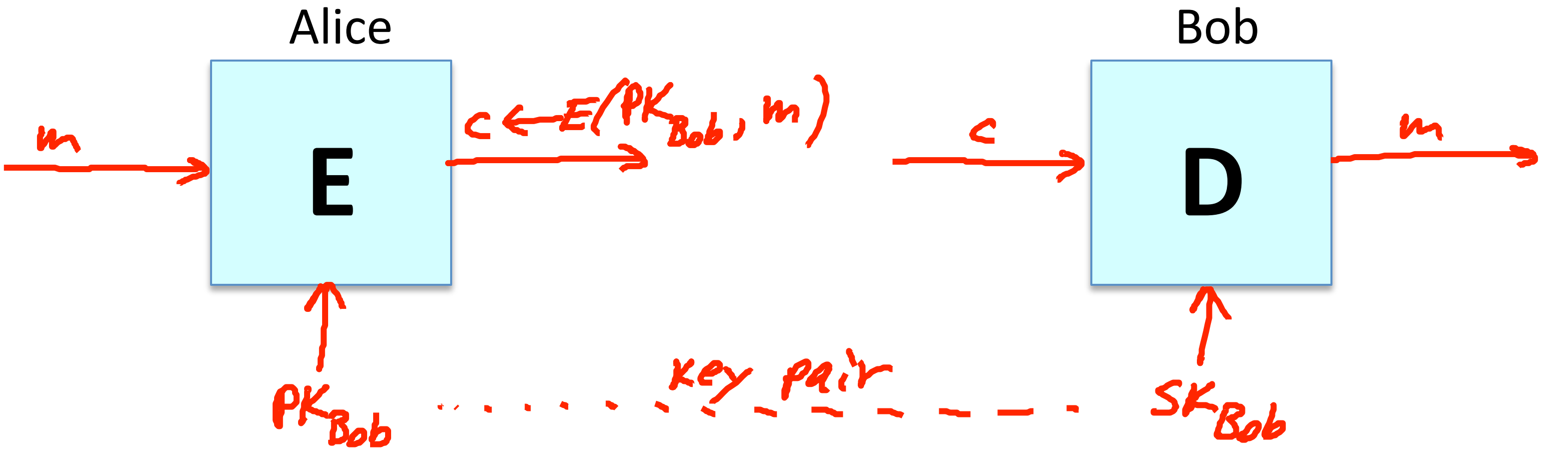
Goal: Alice and Bob want shared secret, unknown to eavesdropper

- For now: security against eavesdropping only (no tampering)



This segment: a different approach

Public key encryption



PK: public key, SK: secret key

Public key encryption

<u>Def</u>: a public-key encryption system is a triple of algs. (G, E, D)

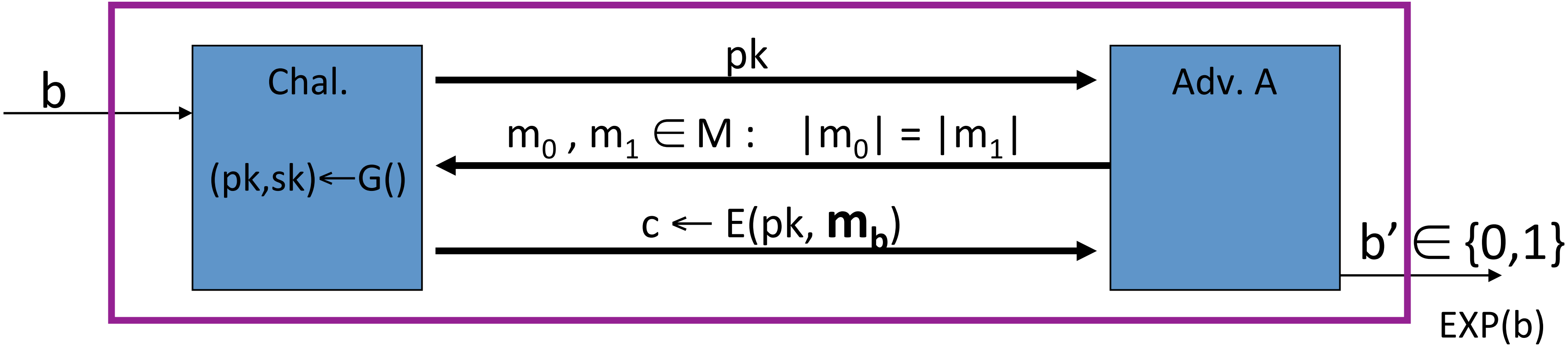
- G(): randomized alg. outputs a key pair (pk, sk)
- E(pk, m): randomized alg. that takes $m \in M$ and outputs $c \in C$
- D(sk,c): det. alg. that takes $c \in C$ and outputs $m \in M$ or $\perp$

Consistency: $\forall$(pk, sk) output by G :

$$\forall m \in M: \quad D(sk, E(pk, m)) = m$$

Semantic Security

For b=0,1 define experiments EXP(0) and EXP(1) as:



Def: $\mathbb{E}$ =(G,E,D) is sem. secure (a.k.a IND-CPA) if for all efficient A:

$$\mathrm{Adv}_{SS}[A,\mathbb{E}] = \left| \Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1] \right| < \text{negligible}$$

Establishing a shared secret

Alice **Bob**

(pk, sk) ⟵ G()

"Alice", pk $\longrightarrow$

choose random
$x \in \{0,1\}^{128}$

"Bob", $c \leftarrow E(pk, x)$ $\longleftarrow$

$D(sk, c) \rightarrow x$

x: shared secret

Security (eavesdropping)

Adversary sees **pk, E(pk, x)** and wants $x \in M$

Semantic security $\Rightarrow$

adversary cannot distinguish

$\{ pk,\ E(pk, x),\ x \}$ from $\{ pk,\ E(pk, x),\ rand \in M \}$

$\Rightarrow$ can derive session key from x.

Note: protocol is vulnerable to man-in-the-middle

Insecure against man in the middle

As described, the protocol is insecure against **active** attacks

Alice	**MiTM**	**Bob**
$(pk, sk) \longleftarrow G()$	$(pk', sk') \longleftarrow G()$	

“Alice”, pk $\longrightarrow$ | "Alice", pk' $\longrightarrow$

choose random
$x \in \{0,1\}^{128}$

$\longleftarrow$ “Bob”, $E(pk, x)$ | $\longleftarrow$ “Bob”, $E(pk', x)$

Public key encryption: constructions

Constructions generally rely on hard problems from number theory and algebra

Next module:

- Brief detour to catch up on the relevant background

Further readings

- Merkle Puzzles are Optimal,
  B. Barak, M. Mahmoody-Ghidary, Crypto ’09

- On formal models of key exchange (sections 7-9)
  V. Shoup, 1999

End of Segment