Lecture 10: public key encryption

Recap: $G = (G, \cdot)$ is a finite cyclic group of prime order q and generator $g \in G$ if $(G, \cdot)$ is a group and $G = \{1, g, g^2, \dots, g^{q-1}\}$ note: $g^\alpha \cdot g^\beta = g^{(\alpha+\beta) \bmod q}$

- CDH assump. in G: $\forall$ "eff" $\mathcal{A}$: $\Pr[\mathcal{A}(g, g^\alpha, g^\beta) = g^{\alpha\beta}] <$ "neg"
- DLOG — " — : — " — $\Pr[\mathcal{A}(g, g^\alpha) = \alpha] <$ "neg"

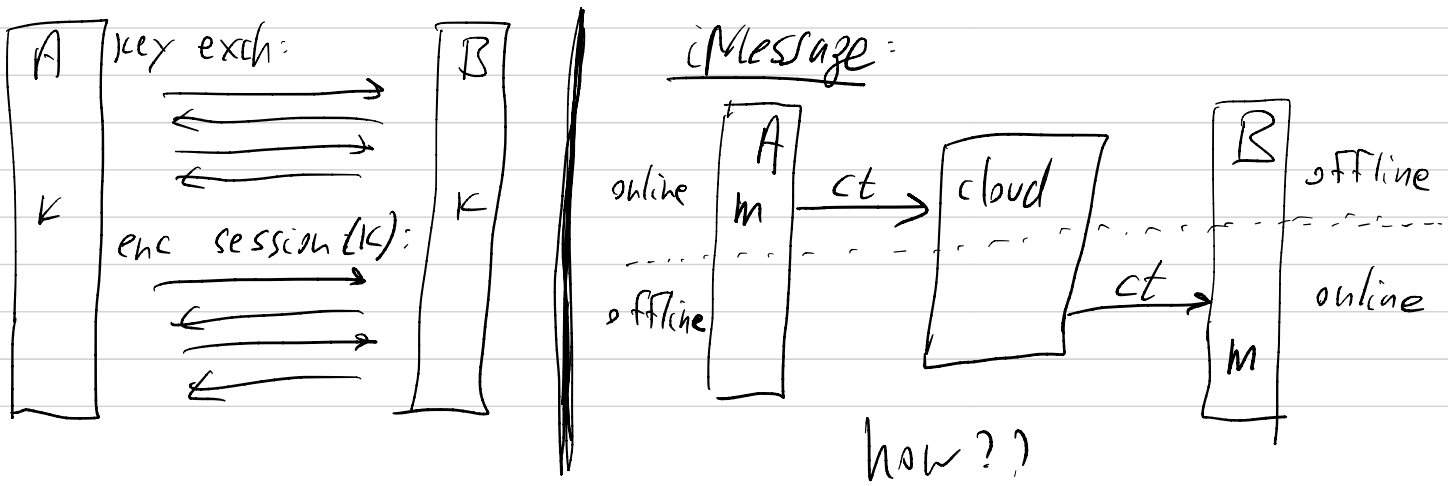
where $\alpha, \beta \xleftarrow{R} \mathbb{Z}_q$.

[examples: (1) $G \subseteq \mathbb{Z}_p^*$ for prime p
(2) G: the group of points of an elliptic curve over $\mathbb{F}_p$.

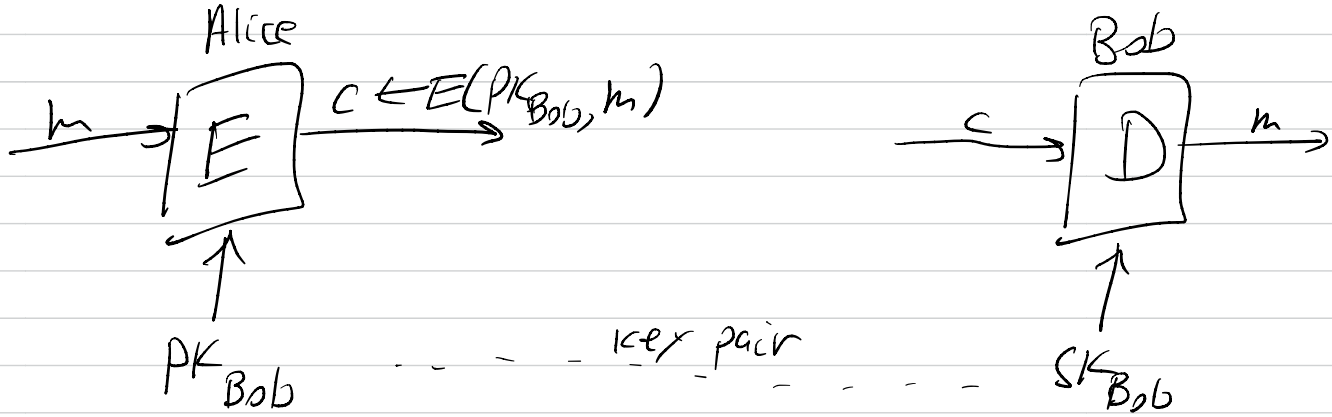
CDH hard in G $\Rightarrow$ D-H key exchange in G.
(secure against eavesdropping)

Two settings: interactive vs. non-interactive

TLS:



Public key encryption (PKE)



PK: public key

SK: secret key

<u>Def</u>: a <u>public key enc.</u> scheme over $(\mathcal{M}, \mathcal{C})$ is a triple of algs. (Gen, E, D)

- $Gen() \to (PK, SK)$: randomized alg. outputs key pair.
- $E(PK, m) \to c$: —"— alg.
- $D(SK, c) \to m$ or reject : det. alg.

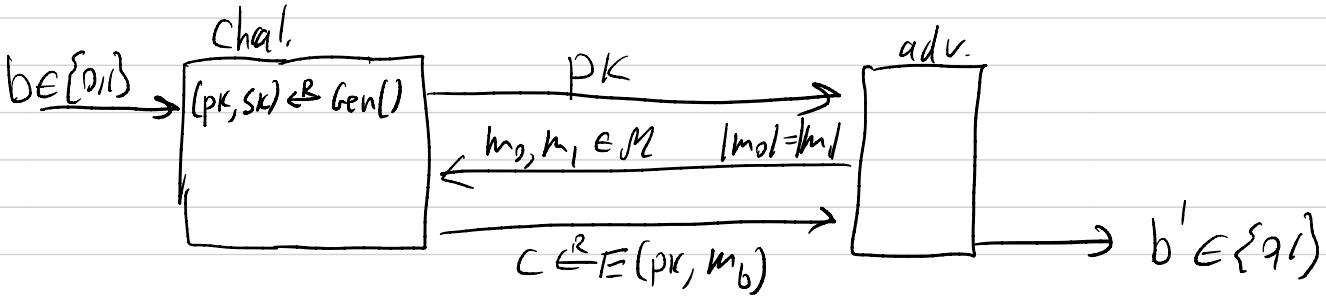
s.t. if $(PK, SK) \xleftarrow{R} Gen()$ then $\forall m \in \mathcal{M}$

$$\Pr[D(SK, E(PK, m)) = m] = 1.$$

<u>note</u>: recipient doesn't know who sent m.

Semantic security (security against eavesdropping)

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



Def: $\mathcal{E} = (G, E, D)$ is <u>sem. secure</u> if $\forall$ "eff" $\mathcal{A}$:

$$Adv_{SS}[\mathcal{A}, \mathcal{E}] := \left| \Pr[EXP(0) = 1] - \Pr[EXP(1) = 1] \right| < \text{"neg"}$$

note: sem. secure PKE $\Rightarrow$ alg. E must be randomized
(if E is deterministic, $\mathcal{E}$ cannot be sem. secure)

Chosen ciphertext security (CCA security):
- security against active attacks
- next time...

Toy key exchange from PKE (secure against eavesdropping)

Alice		Bob
$(pk, sk) \leftarrow Gen()$		
	$\xrightarrow{\quad pk \quad}$	
		$\boxed{k} \xleftarrow{R} \mathcal{M}$
	$\xleftarrow{\quad c \leftarrow E(pk, m) \quad}$	
$D(sk, c) \rightarrow \boxed{k}$		

k: shared secret

security: eavesdropper sees $\boxed{pk, E(pk, k)}$ and want k

Sem sec $\Rightarrow$ $\mathcal{A}$ cannot dist. $(pk, E(pk, k))$ from $(pk, E(pk, 0))$

$\Rightarrow$ $\mathcal{A}$ learns nothing about k.

Insecure against person-in-the-middle

A	PiTM	B
$(pk, sk) \xleftarrow{R} Gen()$	$(pk', sk') \xleftarrow{R} Gen()$	
$\xrightarrow{\quad pk \quad}$	$\xrightarrow{\quad pk' \quad}$	$k \xleftarrow{R} \mathcal{M}$
$\xleftarrow{\quad E(pk, k) \quad}$	$\xleftarrow{\quad E(pk', k) \quad}$	
$\Downarrow$	$\Downarrow$	$\Downarrow$
k	k	k

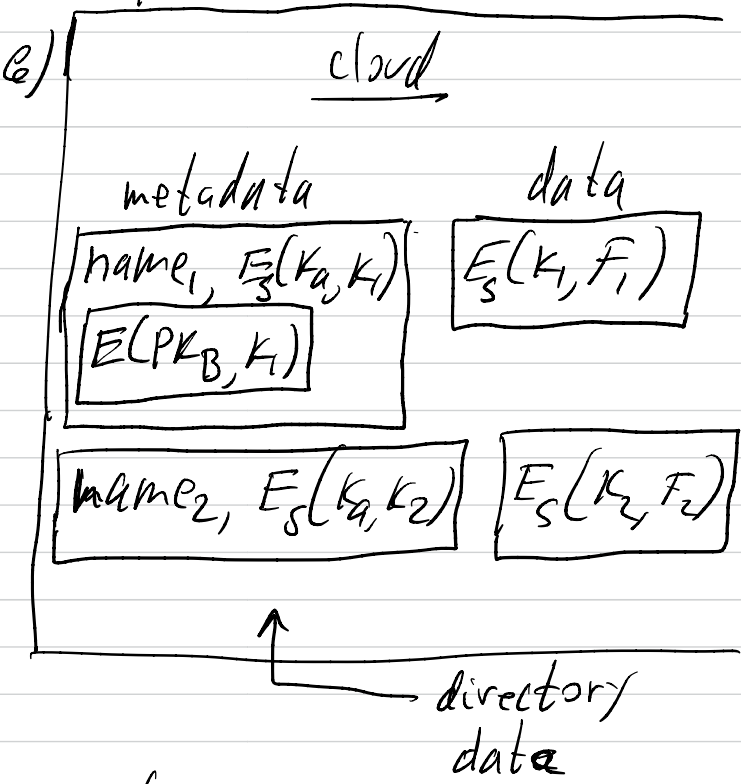
Another app: File sharing in an encrypted file system

(E_s, D_s) : sym. cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

(G, E, D) : PKE

- Alice has $k_a \xleftarrow{R} \mathcal{K}$.
- Alice uploads file F_1 to cloud:

$$\begin{cases} k_1 \xleftarrow{R} \mathcal{K}. \\ \text{compute } E(k_a, k_1),\ E(k_1, F_1) \\ \text{upload.} \end{cases}$$



- Alice uploads file F_2 to cloud:
- Alice wants to give Bob access to F_1

$$\begin{cases} \cdot \text{ get } PK_B \text{ from cloud (how? - later)} \\ \cdot \text{ upload } E(PK_B, k_1) \text{ to cloud.} \\ \cdot \text{ now Bob can read/write } F_1. \end{cases}$$

Note: no interaction with Bob!

- Alice is using PK_B to "send" k_1 to Bob.
- <u>EFS</u>: Alice can give access up to 128 users per file.

Constructing PKE: ElGamal encryption (1982, Stanford)

PKE from D-H.

Ingredients:

- $\mathbb{G}$: Finite cyclic group of order q with gen. $g \in \mathbb{G}$ ($\mathbb{Z}_p^*$ or ell. curve)
- (E_s, D_s): sym. cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$
- $H: \mathbb{G}^2 \to \mathcal{K}$ a hash function.

Gen(): $\alpha \xleftarrow{R} \mathbb{Z}_q$, $h := g^\alpha$, $sk := \alpha$, $pk := h \in \mathbb{G}$

E(pk, m): ($pk = h$) $\beta \xleftarrow{R} \mathbb{Z}_q$, $u := g^\beta$, $v := h^\beta$ $(= g^{\alpha\beta})$

$k := H(u, v) \in \mathcal{K}$ ← key derived from DH secret

$c := E_s(k, m)$

output (u, c)

u	c
hdr	data

D(sk, (u, c)): ($sk = \alpha$) $v := u^\alpha$ $(= g^{\alpha\beta})$

$k := H(u, v) \in \mathcal{K}$

$m := D_s(k, c)$

output m

performance: enc: 2 exp. dec: 1 exp.

as a standard: ECIES (ell. curve integrated enc. system)

Security:

Thm 1: (Gen, E, D) is <u>sem. secure</u> ← eavesdropping security

assuming (1) CDH holds in (G, g),

(2) (E_S, D_S) is sem. secure, and

(3) H is a secure key derivation function (preserves entropy of v)

Thm 2: (Gen, E, D) is <u>CCA seure</u> ← security against tampering attacks (next time)

assuming (1) <u>Interactive DH</u> holds in (G, g) (stronger variant of CDH),

(2) (E_S, D_S) provides Auth. Enc., and

(3) H is a "random oracle".