EECS 575: Advanced Cryptography
Fall 2021
Lecture 15

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- “Wrapping up” symmetric-key cryptography
- Public-key encryption (PKE)
  - IND-CPA security for PKE
- PKE from Diffie-Hellman
- PKE from trapdoor permutations

Agenda for this lecture

- Announcements
- Recap from last time
- “Wrapping up” symmetric-key cryptography
- Public-key encryption (PKE)
  - IND-CPA security for PKE
- PKE from Diffie-Hellman
- PKE from trapdoor permutations

Announcements

- HW5 is online, due 11/8
- Exams are ~~(still) about~~ half-graded

more than!

* very, very subtle exam question
  - Anthony will discuss on Friday
  - very easy grading for q3

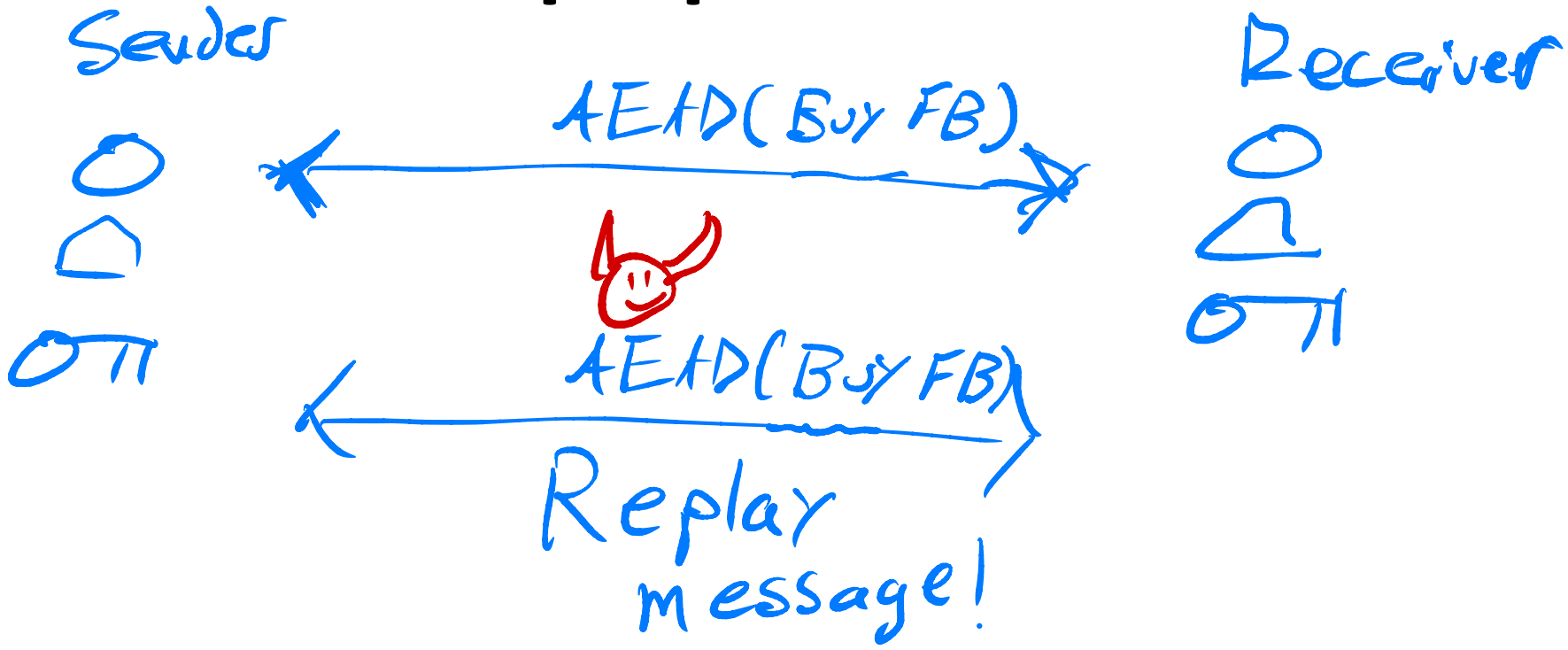
Recap from last time

* Authenticated encryption (with associated data)
* Generic composition
  EG M ⊄ M t E, < E t M
* "Real" AEAD in practice
  Galois/counter mode

Agenda for this lecture

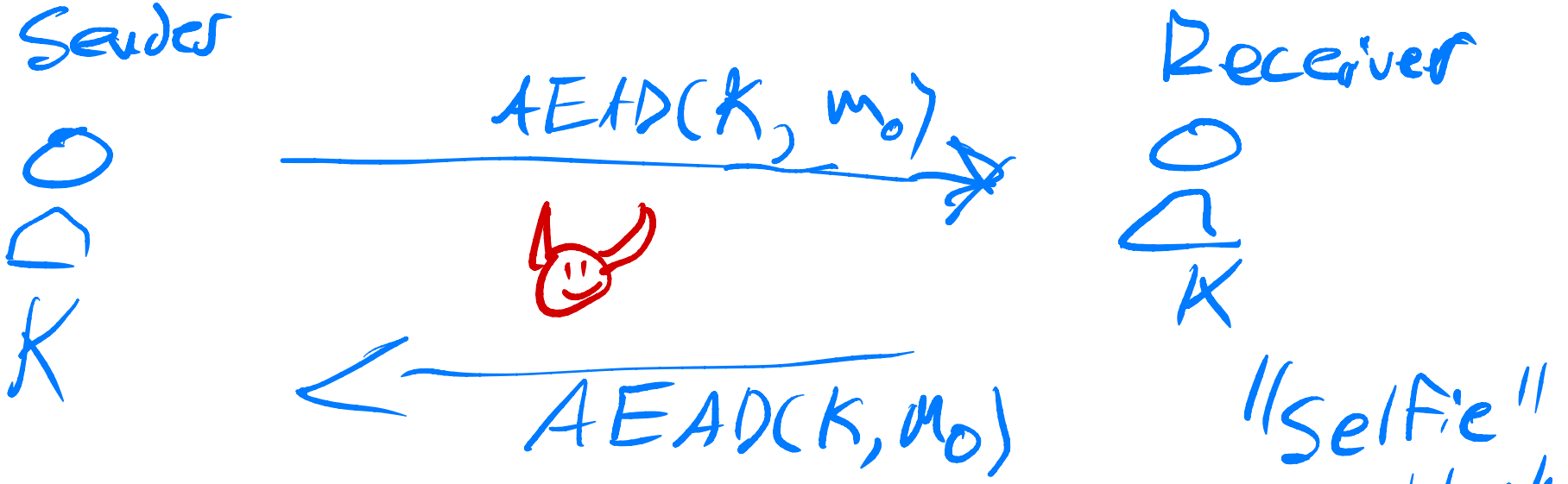
- Announcements
- Recap from last time
- “Wrapping up” symmetric-key cryptography
- Public-key encryption (PKE)
  - IND-CPA security for PKE
- PKE from Diffie-Hellman
- PKE from trapdoor permutations

"Wrap-up" of SKE



"Wrap-up" of SKE

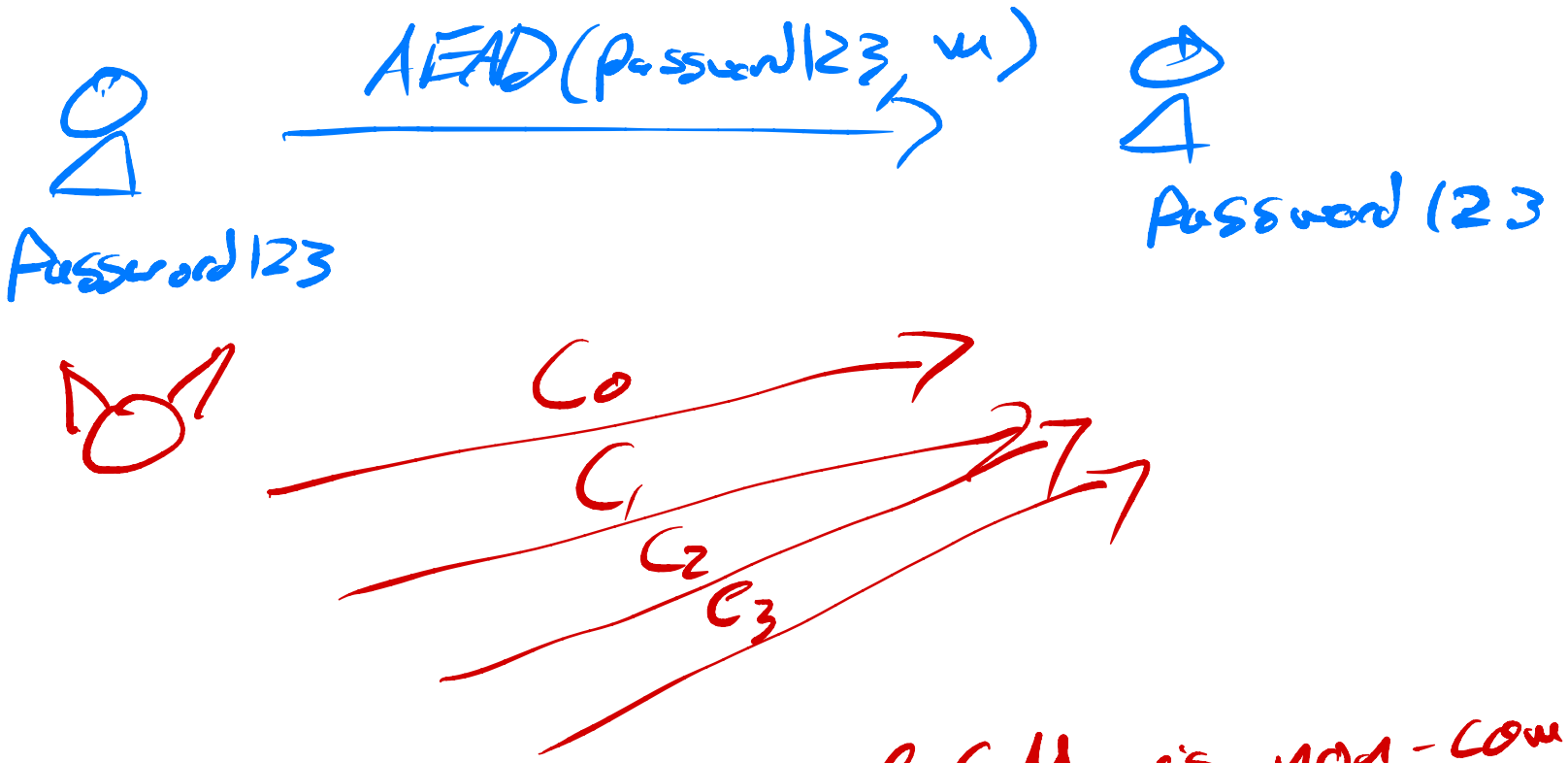
use same key for $S \to R$, $R \to S$



"Selfie" attack

Even if replays prevented, can "reflect" traffic

"Wrap-up" of SKE



Receiver behavior reveals key w/ non-committing AE,

GCM is non-committing GLR'17

learn |D| in log|D|

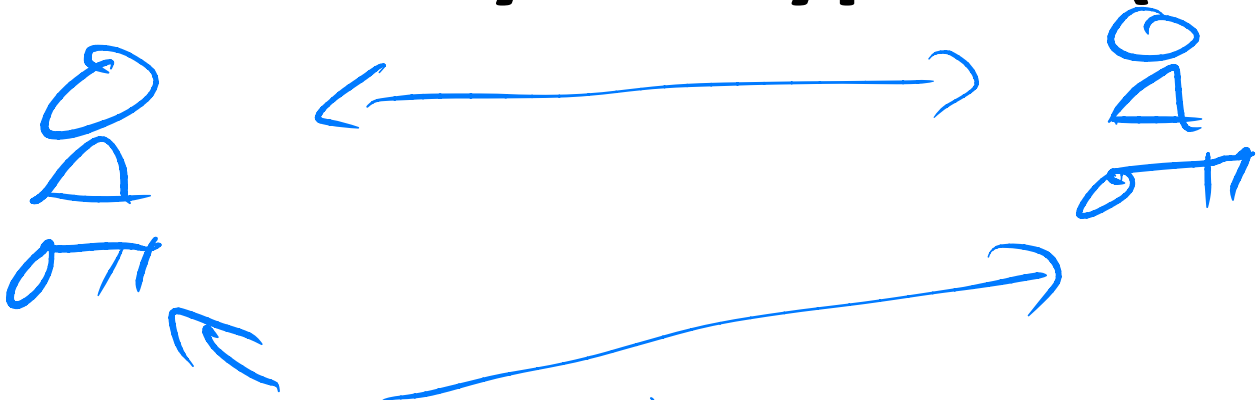
"Wrap-up" of SKE

Wrap up: Take my 498/598 in W22!!

Agenda for this lecture

- Announcements
- Recap from last time
- “Wrapping up” symmetric-key cryptography
- Public-key encryption (PKE)
  - IND-CPA security for PKE
- PKE from Diffie-Hellman
- PKE from trapdoor permutations

Public-key encryption (PKE)

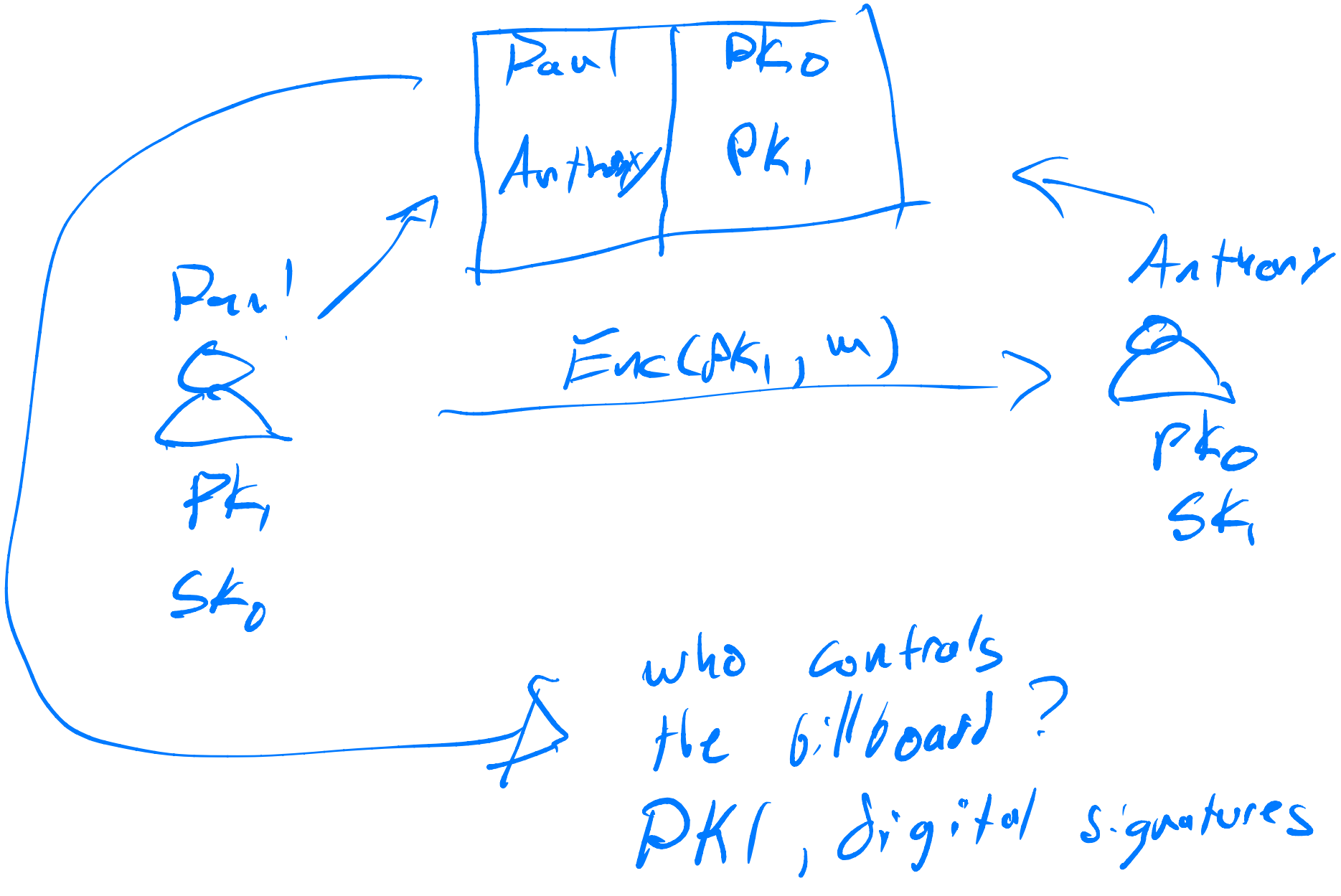


Public-key encryption: "split" key into two

Public key: Can be public. Useful for encryption

Private key: only useful for decryption

Public-key encryption (PKE)



Public-key encryption (PKE)

* Gen: outputs (pk, sk)
* Enc: takes pk, m, outputs $ct \in \mathbb{C}$
* Dec: takes sk, ct, outputs $m \in \mathcal{M}$ (or $\perp$)

IND-CPA security

$\underline{CPA^0(A):}$

$(PK, SK) \leftarrow Gen$

$b \leftarrow A^{C^0(\cdot,\cdot)}(PK)$

$\underline{C^0(m_0, m_1):}$

Ret $Enc_{PK}(m_0)$

$\underline{CPA^1(A):}$

$(PK, SK) \leftarrow Gen$

$b \leftarrow A^{C^1(\cdot,\cdot)}(PK)$

$\underline{C^1(m_0, m_1):}$

Ret $Enc_{PK}(m_1)$

$$Adv^{CPA}_{PKE}(A): \left| Pr[CPA^0(A) = 1] - Pr[CPA^1(A) = 1] \right|$$

PKE is IND-CPA secure if $Adv^{CPA}_{PKE}(A) = negl(n)$ $\forall$ nuppt A

Agenda for this lecture

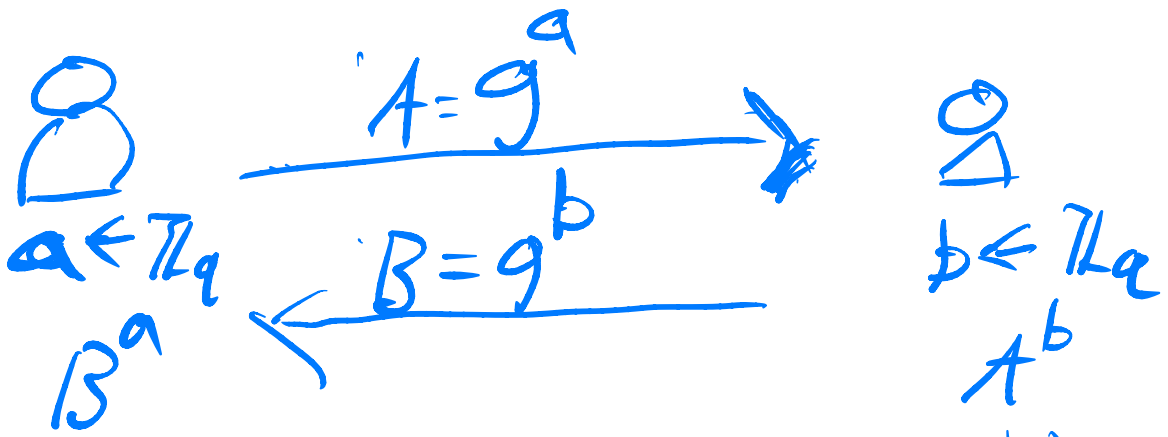
- Announcements
- Recap from last time
- “Wrapping up” symmetric-key cryptography
- Public-key encryption (PKE)
  - IND-CPA security for PKE
- PKE from Diffie-Hellman
- PKE from trapdoor permutations

PKE from Diffie-Hellman key exchange

Diffie-Hellman:

"ElGamal"

Group $G = \langle g \rangle$ of order q



Secure when computing g^{ab} from g^a, g^b is hard.

computational Diffie-Hellman

Better: g^{ab} looks random, even given g^a, g^b

Decisional Diffie-Hellman

PKE from Diffie-Hellman key exchange

DDH: Let $G = \langle g \rangle$ of order q,

$$(g, g^a, g^b, g^{ab}) \approx_c (g, g^a, g^b, g^c)$$

not random! random element

For $a, b, c \leftarrow \mathbb{Z}_q$

Does DDH hold in $\mathbb{Z}_p^*$? NO

g^{ab} ← even w.p. 3/4

g^c ← even w.p. 1/2

- is a group,
- order $p-1$,
- cyclic
- can learn whether z is odd/even given g^z

In practice: $p = 2q+1$ for prime q, work in QR_p^*

PKE from Diffie-Hellman key exchange "Elgamal"

Group $G = \langle g \rangle$, order q

* Gen: $a \leftarrow \mathbb{Z}_q$, $pk = g^a$, $sk = a$

Return (pk, sk)

Sender's DH value

Receiver's DH group op

$M = G$ * Enc(pk, m): $r \leftarrow \mathbb{Z}_q$, $R \leftarrow g^r$, $c \leftarrow (pk)^r \cdot m$

Returns (R, c)

shared secret looks random

* Dec$(sk, (R', c'))$:

Returns $c' / (R')^{sk}$

IND-CPA follows by DDH in G. Exercise

Trapdoor permutations (TDPs)

OWP family with trapdoor

* $S(1^n)$: index for function, s — allows computing f_s^{-1}
  trapdoor for inverting, $t \leftarrow$
* OWP w.r.t S

---

* Gen: $(s,t) \leftarrow S(1^n)$. Ret $pk = s$, $sk = t$
* $Enc(pk, m)$: $r \leftarrow D_s$; Ret $(f_s(r), h(r) \oplus m)$
* $Dec(sk, (R, c))$: Ret $h(f_s^{-1}(R)) \oplus c$

$\{0,1\}^\ell \leftarrow$

Compute with t/sk

Secure because $h(r)$ is pseudorandom.

PKE from TDPs