EECS 575: Advanced Cryptography
Fall 2022
Lecture 16

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

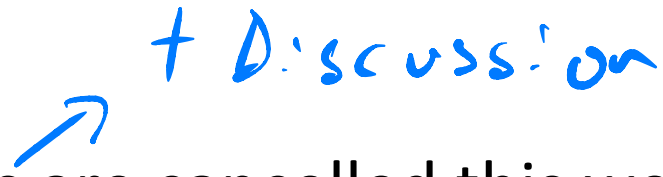
- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Announcements

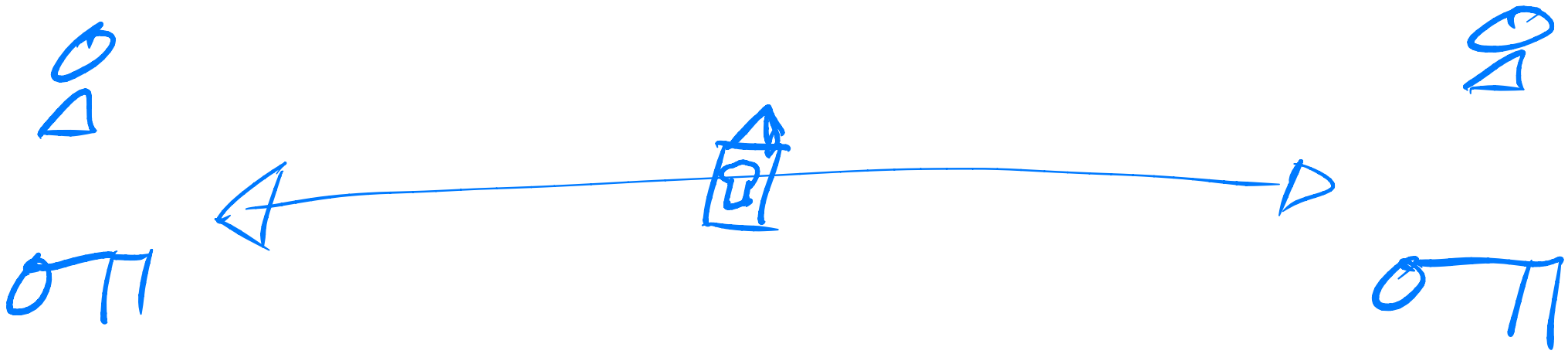
- HW4 is out, due 11/7
- Alexandra's office hours are cancelled this week
  - I will host extra OH to make up for her absence; time TBD (Piazza)



Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Authenticated Encryption



- replay attacks
- Communication volume
- Forward secrecy / post-compromise
- More!

Authenticated Encryption

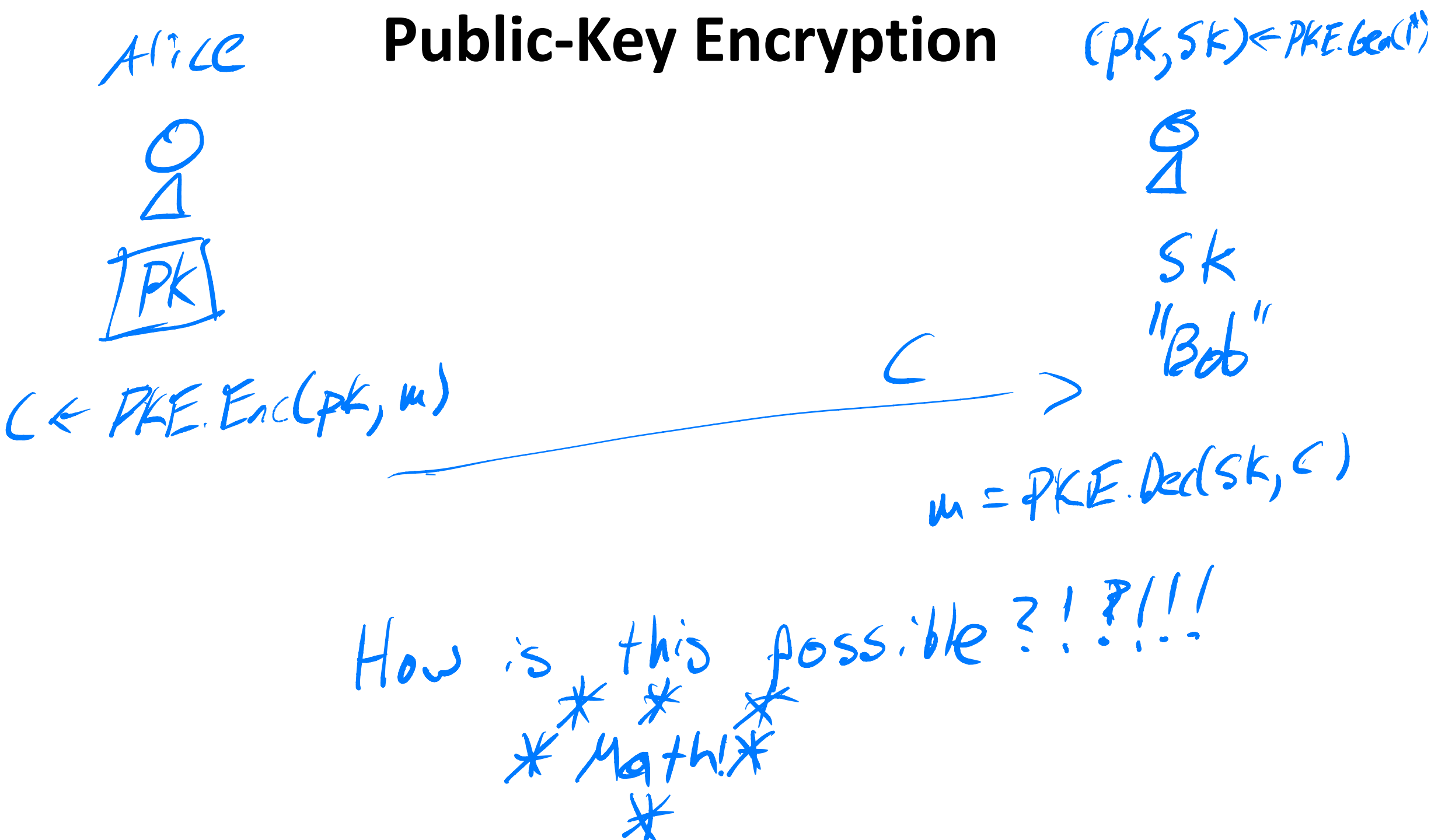
How to agree on a shared secret?

Public-key encryption!

Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Public-Key Encryption



IND-CPA for PKE

$\underline{IND\text{-}CPA0^A:}$
$K \leftarrow Gen$
$b \leftarrow A^{Enc(\cdot),\, C_0(\cdot,\cdot)}$

$\underline{C_0(m_0, m_1):}$
$Ret\ Enc(K, m_0)$

$\underline{IND\text{-}CPA1^A:}$
$K \leftarrow Gen$
$b \leftarrow A^{Enc(\cdot),\, C_1(\cdot,\cdot)}$

$\underline{C_0(m_0, m_1):}$
$Ret\ Enc(K, m_1)$

Q: Can IND-CPA PKE be deterministic?

A: No.

$\underline{IND\text{-}CPA0^A:}$
$(pk, sk) \leftarrow PKE.Gen$
$b \leftarrow A^{C_0(\cdot,\cdot)}(pk)$

$\underline{C_0(m_0, m_1):}$
$Ret\ PKE.Enc(pk, m_0)$

$\underline{IND\text{-}CPA1^A:}$
$(pk, sk) \leftarrow PKE.Gen$
$b \leftarrow A^{C_1(\cdot,\cdot)}(pk)$

$\underline{C_1(m_0, m_1):}$
$Ret\ PKE.Enc(pk, m_1)$

IND-CPA for PKE

Exercise:

Thm: If IND-CPA PKE for one-bit msgs exists, then IND-CPA PKE for poly(n)-bit msgs exists.

Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Background on group theory

Group $G = \{S, \cdot\}$

operation has
- identity: $\forall S, \exists e$ s.t. $e \cdot x = x$
- inverses: $\forall x \in S, \exists y \in S$ s.t. $x \cdot y = e$
- associative $\forall x, y, z$ $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

Order of group: $|S|$

Fact: $x \in S$

$$\underbrace{x}^{|S|} = e$$

$$\underbrace{x \cdot x \cdot \ldots \cdot x}_{|S|}$$

E.g. Z_N^*, Z_p^*

Elliptic curve group $\rightarrow y^2 = x^3 + ax + b$ mod p

(x, y) satisfying equ

Background on group theory

Cyclic group. G is cyclic if $\exists g$ s.t.

$$G = \{g^0, g^1, \ldots, g^{|G|-1}\}$$

$\mathbb{Z}_p^*$ is cyclic

Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

Discrete Logarithm Problem

Given X, hard to compute x s.t. $X = g^x$

"discrete logarithm" of X w.r.t. g

Integer between 0 and $|S|-1$

Let $S(1^\lambda) = p, g$. $\forall$ nuPPT $\mathcal{A}$

$$\Pr_{\substack{(p,g) \leftarrow S \\ y \leftarrow \mathbb{Z}_p^*}} [\mathcal{A}(p,g,y) = \log_g y] = \text{negl}(\lambda)$$

Diffie-Hellman Problem(s)

Cyclic group G w/ generator g, $ord(G) = q$

Hard to compute g^{ab} given

$$(g, g^a, g^b)$$

"computational" DH assumption

Decisional DH assumption:

$a, b, c \leftarrow \{0, \ldots, q-1\}$

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

Diffie-Hellman Problem(s)

$H_\infty(g^{ab} \mid g^a, g^b) = 0$

$H_\infty(g^c \mid g^a, g^b) = \log \mathrm{ord}(G)$

No entropy at all, but

comp. ind. from uniform random!

Agenda for this lecture

- Announcements
- Recap from last time
- Public-Key Encryption: syntax and security
- Group theory background
- Discrete logarithm and Diffie-Hellman problems
- El Gamal encryption

ElGamal PKE

QR_p^*, g, $ord = \frac{p-1}{2} = q$, $p = 2q+1$, q prime

$\subseteq \mathbb{Z}_p^*$

- Gen: Sample $a \in \mathbb{Z}_q$,
  Set $PK = g^a$ and $SK = a$
  Ret (PK, SK)
- $Enc(pk, m)$ $[m \in QR_p^*]$:
  - Sample $r \in \mathbb{Z}_q$, $R = g^r$
  - $c_0 = R$
  - $c_1 = (PK)^r \cdot m$
  - Ret (c_0, c_1)
- $Dec(sk, (c_0, c_1))$:
  - Compute $T = (c_0)^{SK} = g^{SK \cdot r}$
  - Ret c_1 / T

ElGamal PKE

Thm: If DDH holds in $\mathbb{G}\mathbb{R}_p^*$,
then ElGamal PKE is IND-CPA

Proof: Exercise.

Replace $g^{sk \cdot r}$ with g^e using DDH.

Argue ctxt is indep. of message m_0/m_1.