CSE 575: Advanced Cryptography
Fall 2024
Lecture 13

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

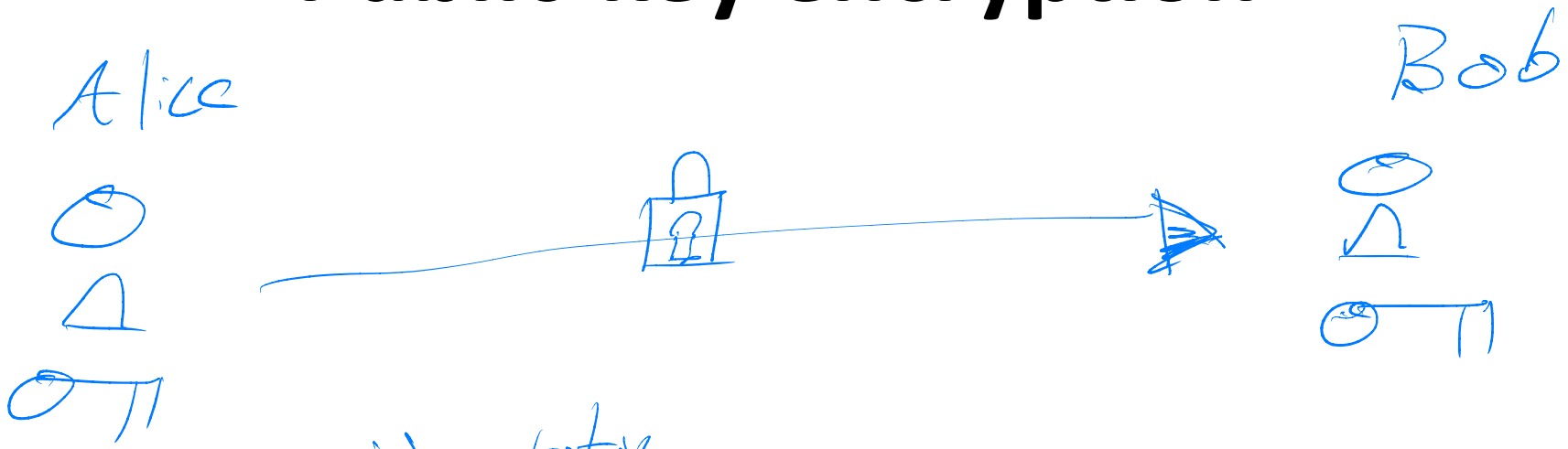
Announcements

- Midterm out, due 10/11

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

Public-key encryption



- identity
- replay attacks
- Communication volume
- key compromise
- key exchange

Public-key encryption

History of PKE

- Diffie - Hellman — Turing award '76 — Key exchange
- Rivest - Shamir - Adleman — Turing award — PKE '77
- Clifford Cocks — GCHQ — Public talks in 70s ?

- NSA pressure
- export controls

Public-key encryption

Syntax

- Gen: return (pk, sk)
  - pk: Public key
  - sk: secret key
- Enc(pk, m): Ret c
  - anyone can run
- Dec(sk, c): Ret m
  - only sk holder can run

Correctness

$$\Pr[\mathrm{Dec}(sk, \mathrm{Enc}(pk, m)) = m] = 1$$

$(pk, sk) \leftarrow \mathrm{Gen}$

randomness in encrypt

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

IND-CPA for PKE

$\underline{IND\text{-}CPA^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow PKE.Gen$

$b \leftarrow \mathcal{A}^{\mathcal{C}_0(\cdot,\cdot)}(pk)$

Ret b

$\underline{\mathcal{C}_0(m_0, m_1)}$:

Ret $PKE.Enc(pk, m_0)$

$\underline{IND\text{-}CPA^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow PKE.Gen$

$b \leftarrow \mathcal{A}^{\mathcal{C}_1(\cdot,\cdot)}(pk)$

Ret b

$\underline{\mathcal{C}_1(m_0, m_1)}$:

Ret $PKE.Enc(pk, m_1)$

PKE is IND-CPA if: $\forall$ nuPPT $\mathcal{A}$

$$\left| Pr[IND\text{-}CPA^{\mathcal{A}}_{PKE} = 1] - Pr[IND\text{-}CPA^{\mathcal{A}}_{PKE} = 1] \right| = negl(\lambda)$$

IND-CPA for PKE

Thm: If $\exists$ IND-CPA PKE for 1-bit msgs,
then $\exists$ IND-CPA PKE for poly(n)-bit msgs.

Proof: Exercise.
encrypt one bit at a time,
use hybrid argument.

Q: True for SKE? Caveats?

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

Cyclic
Abelian

Group theory background

Group: (set X and binary operation $\cdot$)

- identity element $\exists e$ s.t. $\forall a$

$$a \cdot e = a$$

- inverses: $\forall x \exists y$ s.t.

$$xy = e$$

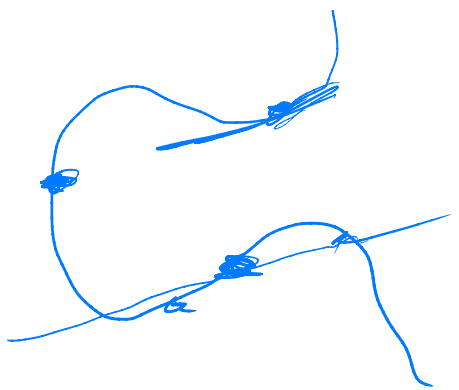
- $\forall a, b, c$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- commutes: $\forall a, b$,

$$a \cdot b = b \cdot a$$

- Cyclic: $\exists g$ s.t. $\{g^0, g^1, \ldots, g^{p-1}\} = X$



$(x, y) \in \mathbb{F}_p$

$$y^2 = x^3 + ax + b$$

$$|E/\mathbb{F}_p| \approx p \pm \sqrt{p}$$

E.g. $\mathbb{Z}_N^*$ $N = pq$ $\mathbb{Z}_p^*$ elliptic curve group

Hardness assumptions for groups

Discrete log

Let $S(1^n) = p, g$ output group $G = \langle g \rangle$ of order p

$\forall$ n.u. PPT A,

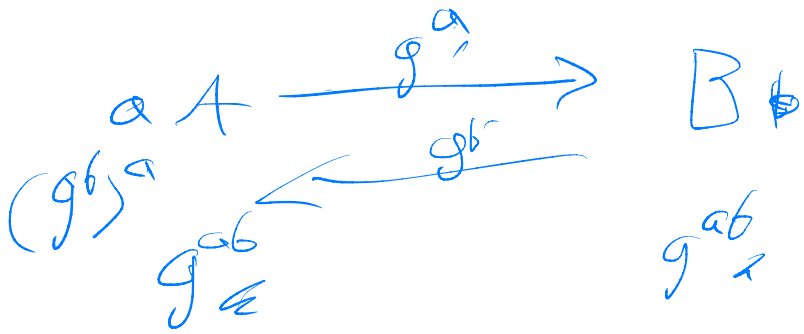
$$\Pr\left[A(p, g, y) = x \text{ s.t. } g^x = y\right] = \text{negl}(n)$$

$y \leftarrow G$

Computational D-H:

$\forall$ n.u. PPT A,

$$\Pr_{a,b \leftarrow \mathbb{Z}_p}\left[A(g, p, g^a, g^b) = g^{ab}\right] = \text{negl}(n)$$



Hardness assumptions for groups

Decisional D-H

$a, b, c \in \mathbb{Z}_p$

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

Entropy of g^c conditioned on g^a, g^b ?

|| || g^{ab} || ...

Agenda for this lecture

- Announcements
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions
- Elgamal encryption

Elgamal PKE

$G = \langle g \rangle$ of order p

- Gen:
  $x \leftarrow \mathbb{Z}_p$
  Ret (g^x, x)
- Enc(pk, m):
  $r \leftarrow \mathbb{Z}_p$
  Ret $(g^r, (pk)^r \cdot m)$
- Dec(sk, c_0, c_1):
  Ret c_1 / c_0^{sk} $\Rightarrow$ $c_1 \cdot c_0^{-sk}$

Correctness:

Dec(sk, Enc(pk, m))

$\hookrightarrow$ Dec(x, $(g^r, (g^x)^r \cdot m)$)

$(g^x)^r \cdot m / (g^r)^x = m$

Security: Thm:
If DDH hard in G,
then Elgamal IND-CPA.

Proof:
Exercise

Analyzing Elgamal