COL759:

CRYPTOGRAPHY AND COMPUTER SECURITY

2022-23 (SEMESTER 1)

LECTURE 29: PUBLIC KEY ENC

REVIEW: $\mathbb{Z}_p^*$ and its prime-order subgroup $\mathbb{G}$

$\mathbb{Z}_p^* = \langle g \rangle$ where g : generator of $\mathbb{Z}_p^*$

$\mathbb{Z}_p^*$

$|\mathbb{Z}_p^*| = p - 1 = 2q$

Almost 50% of elements in group are generators of $\mathbb{Z}_p^*$

Common Properties

- contain 1
- Closed under multiplication mod p
- Every element has an inverse

DISCRETE LOG problem : hard

$\mathbb{G} = \langle g^2 \rangle$: prime-order subgroup of $\mathbb{Z}_p^*$

$|\mathbb{G}| = q$

Almost every element in group is a generator of $\mathbb{G}$

Decision Diffie-Hellman problem : hard

REVIEW: DLOG and DDH over prime-order group $\mathbb{G}$

DISCRETE LOG problem

Given random generators (g, h)
compute a such that $h = g^a$

DECISION DIFFIE-HELLMAN problem

Distinguish the following distributions

$\mathscr{D}_0 = \left\{(g, g^a, g^b, g^{a \cdot b})\right\}_{g \leftarrow \mathbb{G},\ a,b \leftarrow \mathbb{Z}_q}$ $\mathscr{D}_1 = \left\{(g, g^a, g^b, g^c)\right\}_{g \leftarrow \mathbb{G},\ a,b,c \leftarrow \mathbb{Z}_q}$

PLAN FOR TODAY'S LECTURE

- A collision resistant hash fn using DLOG
- Intro to public key encryption
- A secure public key enc. scheme using DDH
- Some nice properties of DLOG / DDH

COLLISION RESISTANCE USING PRIME-ORDER GROUP $\mathbb{G}$

Prime order group $\mathbb{G}$ of size q

Hash key: two elements in $\mathbb{G}$

$$H_k : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{G}$$

$$H_{(x,y)}(a, b) = (x^a) \underbrace{\times_p}_{\text{mult mod } p} (y^b)$$

Looks very similar to the insecure construction we saw last time

Goal: H is secure, assuming hardness of DISCRETE LOG

CRHF CONSTRUCTION USING PRIME-ORDER GROUP $\mathbb{G}$

$H_k : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{G}$

$$H_{(x,y)}(a, b) = (x^a) \times_p (y^b)$$

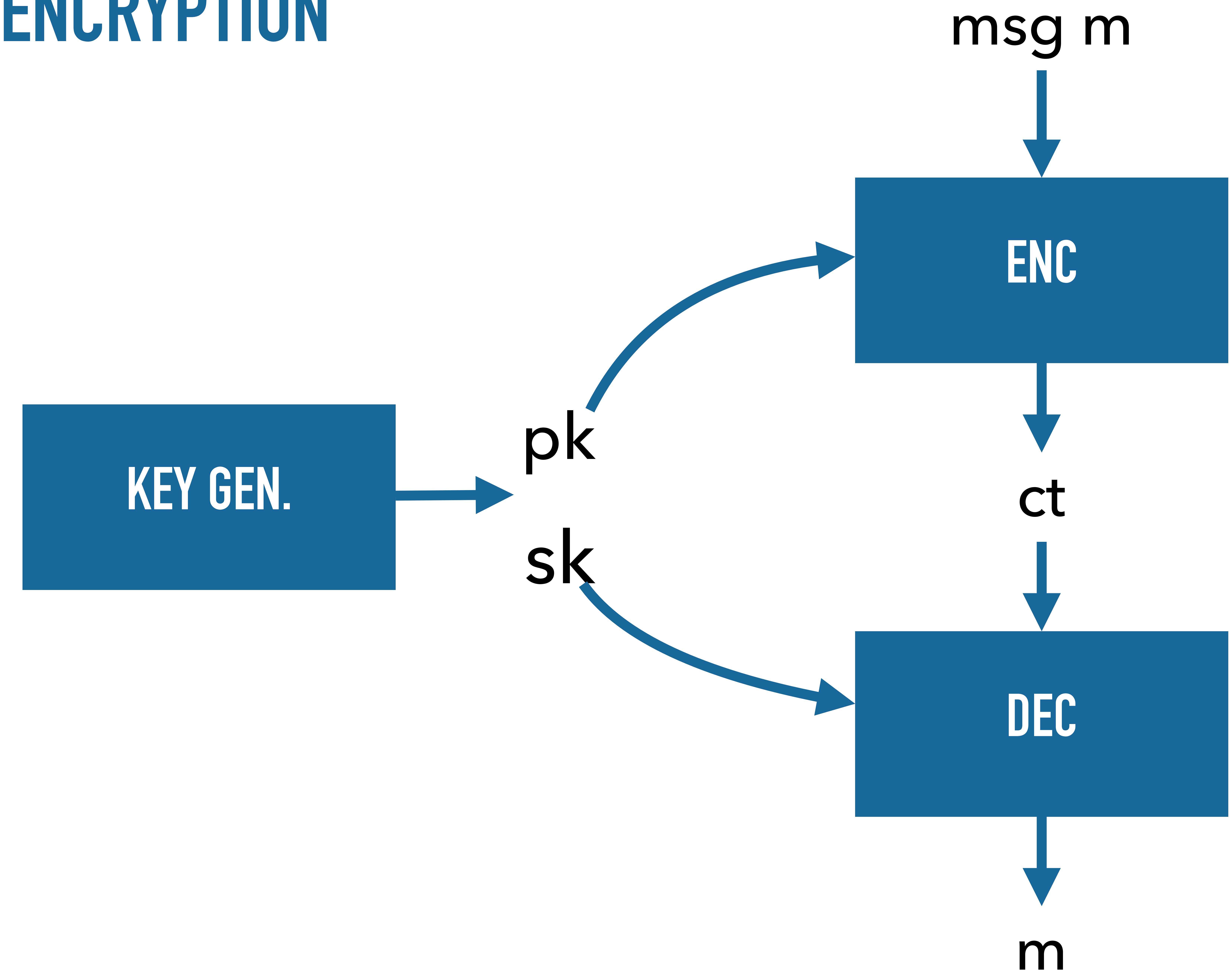
Goal: secure CRHF assuming DLOG

H.W.

Modify previous construction to make it secure, assuming DLOG is hard over $\mathbb{Z}_p^*$

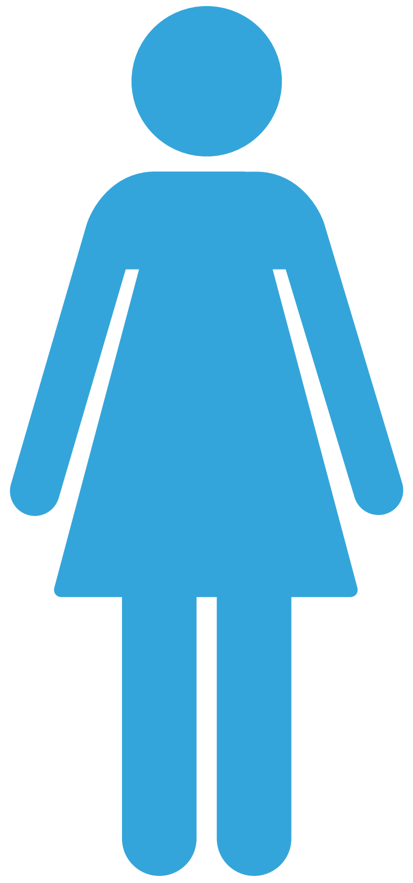

MACs
Auth. Enc.
CRHFs
PRFs
Key Agreement
Commitments
PRGs
DDH over prime order groups
PUBLIC KEY ENCRYPTION

PUBLIC KEY ENCRYPTION



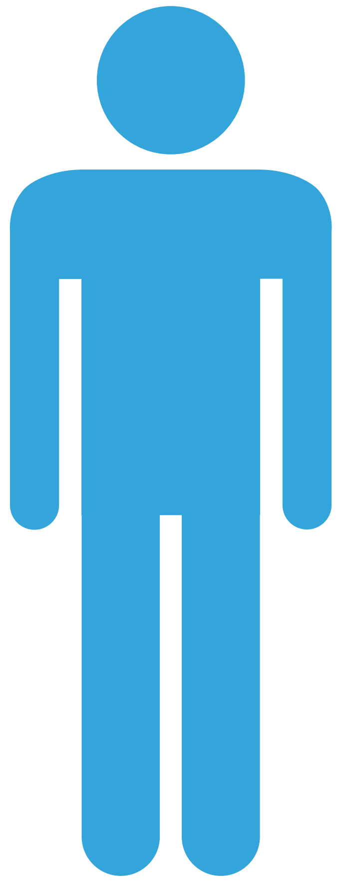
PUBLIC KEY ENCRYPTION

pk: known to everyone



$\mathsf{ct} \leftarrow \mathsf{Enc}(m, pk)$

???



Generates (pk, sk)

Recovers m using Dec(ct, sk)

DEFINING SECURITY FOR PUBLIC KEY ENCRYPTION

Security in the symmetric key setting

PASSIVE SECURITY: ONE-TIME SEMANTIC SECURITY

Chall.		Adv.	
Chooses keys (pk, sk)	$\xrightarrow{\text{pk}}$		Setup
$b \leftarrow \{0,1\}$ $\mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{m}_b^*, pk)$	$\xleftarrow{m_0^* \quad m_1^*}$ $\xrightarrow{\mathsf{ct}^*}$		Chall.
	$\xleftarrow{b'}$		Guess

PASSIVE SECURITY: MANY-TIME SEMANTIC SECURITY

Chall. | Adv.

Setup

Chooses keys (pk, sk)

Chooses bit b

pk

Poly. many Chall. queries

$b \leftarrow \{0,1\}$

$m^*_{i,0}$ $m^*_{i,1}$

$\mathsf{ct}^* \leftarrow \mathsf{Enc}(m^*_{i,b}, pk)$

ct^*_i

Guess

b′

Is many-time semantic security stronger than one-time semantic security?

A natural first guess, based on our symmetric key experience, is that one-time security for PKE is strictly weaker than many-time security for PKE. However, these two notions are equivalent in the PKE setting.

MANY-TIME SEMANTIC SECURITY $\equiv$ ONE-TIME SEMANTIC SECURITY

Key idea: Hybrid technique

ATTACKS NOT CAPTURED BY SEMANTIC SECURITY GAME

'74 - Diffie-Hellman propose key agreement protocol

Introduce the notion of public key encryption

'77 - Rivest-Shamir-Adleman: first PKE scheme

'82 - Goldwasser-Micali: formal definitions of PKE security

'85 - Elgamal: PKE scheme very similar to DH key exchange

DDH-based PKE scheme

Taher Elgamal

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-31, NO. 4, JULY 1985

A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms

TAHER ELGAMAL, MEMBER, IEEE

Abstract—A new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.

I. Introduction

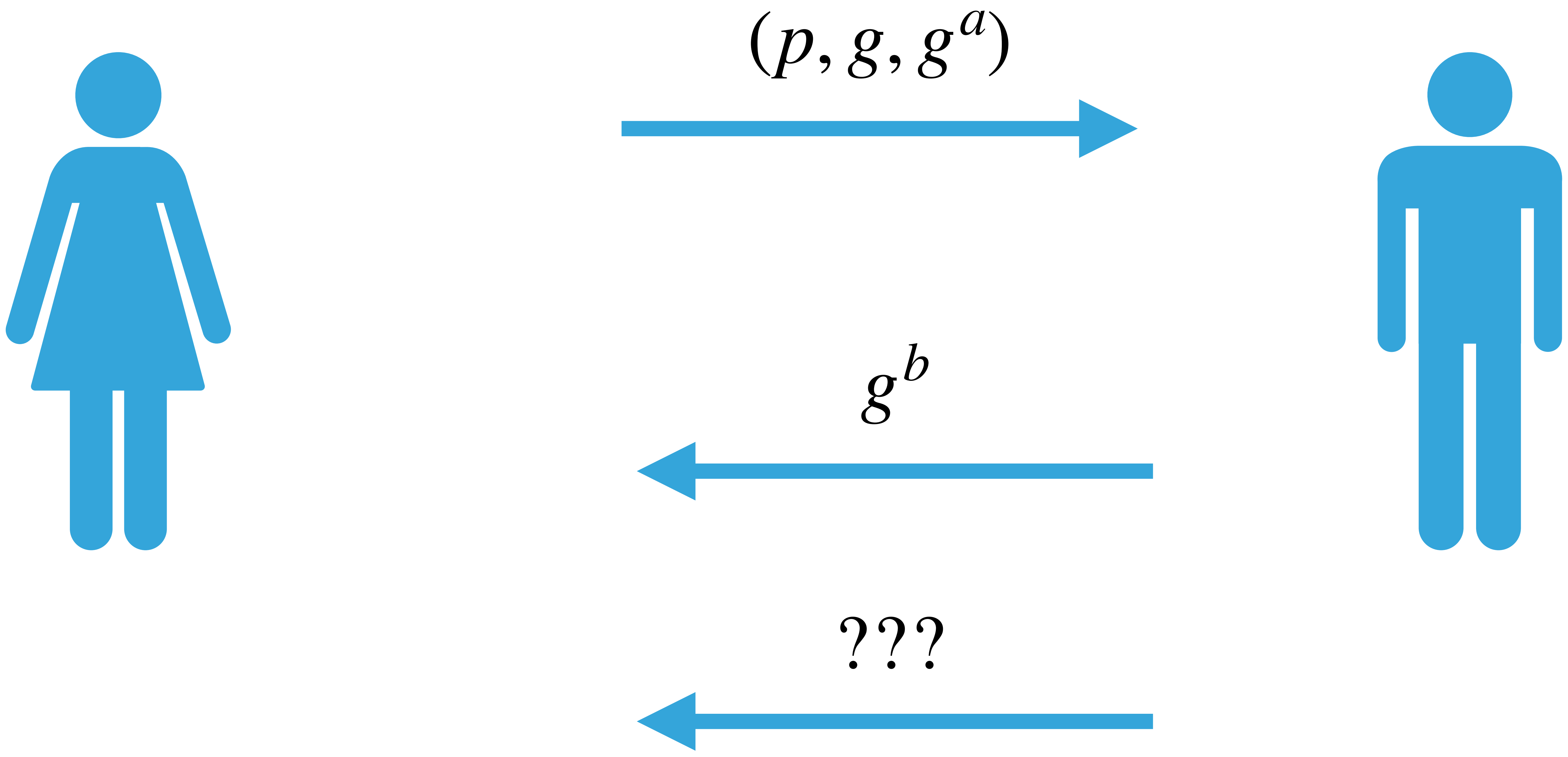
IN 1975, Diffie and Hellman [3] introduced the concept

Hence both A and B are able to computer K_{AB}. But, for an intruder, computing K_{AB} appears to be difficult. It is not yet proved that breaking the system is equivalent to computing discrete logarithms. For more details refer to [3].

In any of the cryptographic systems based on discrete logarithms, p must be chosen such that p - 1 has at least one large prime factor. If p - 1 has only small prime factors

DDH-based PKE scheme: The Elgamal Encryption Scheme

Toy scenario: Bob wants to send exactly one secret message m to Alice



DDH-based PKE scheme: The Elgamal Encryption Scheme

Construction uses prime order group $\mathbb{G} = \langle g \rangle$

Message space: $\mathbb{G}$

Key Generation: $a \leftarrow \mathbb{Z}_q, \quad pk = g^a, sk = a$

Enc (m, pk) : $\quad b \leftarrow \mathbb{Z}_q, \quad ct_1 = g^b, ct_2 = m \cdot (pk)^b$

Dec $((ct_1, ct_2), sk)$: $\quad$ Output $ct_2 \cdot (ct_1^{q-sk})$

H.W.

How to encrypt longer messages?

DDH-based Proof of Security

Exercises

1. Construct a public key encryption scheme with unbounded message space, whose security can be proven assuming the DDH problem is hard.

2. Let $p = 2q + 1$ be a safe prime where $p = \Theta(2^n)$. Assume the Discrete Log problem is hard over prime-order subgroups of $\mathbb{Z}_p^*$ (that is, for any p.p.t. algorithm B, $\Pr[B(h, h^b) = b : h$ is a random element of $\mathbb{Z}_p^*$ s.t. $|\langle h \rangle| = q, b \leftarrow \mathbb{Z}_q] \leq \text{negl}(n))$.

   Show that the Discrete Log problem is also hard over $\mathbb{Z}_p^*$. That is, for any p.p.t. algorithm B, the following probability is also bounded by a negligible function in n: $\Pr[B(g, g^a) = a : g$ is a random generator of $\mathbb{Z}_p^*, \quad a \leftarrow \mathbb{Z}_p]$

   What about the converse?

Exercises

3. Assume DDH is hard over prime-order group $\mathbb{G}$. Show that the following distributions are indistinguishable:

$$\mathscr{D}_0 = \left\{(g, g^a, g^b, g^c, g^{a\cdot b}, g^{a\cdot c})\right\}_{g\leftarrow\mathbb{G},\ a,b,c\leftarrow\mathbb{Z}_q} \qquad \mathscr{D}_1 = \left\{(g, g^a, g^b, g^c, g^d, g^e)\right\}_{g\leftarrow\mathbb{G},\ a,b,c,d,e\leftarrow\mathbb{Z}_q}$$

Hint: hybrid technique

4 (**). Let $\mathbb{G}$ be a prime-order group, and suppose there exists a p.p.t. algorithm that can solve the DDH problem with probability 0.51. Discuss how to boost the success probability to 0.99.

Hint: you will need Chernoff's bound for this. As a stepping stone, consider the following simpler problem: you are given a sample, which is either a DDH sample, or a non-DDH sample. Using this sample, generate two independent samples, such that the two samples are DDH samples if and only the original sample was a DDH sample.