Public key cryptography

Hyoungshick Kim

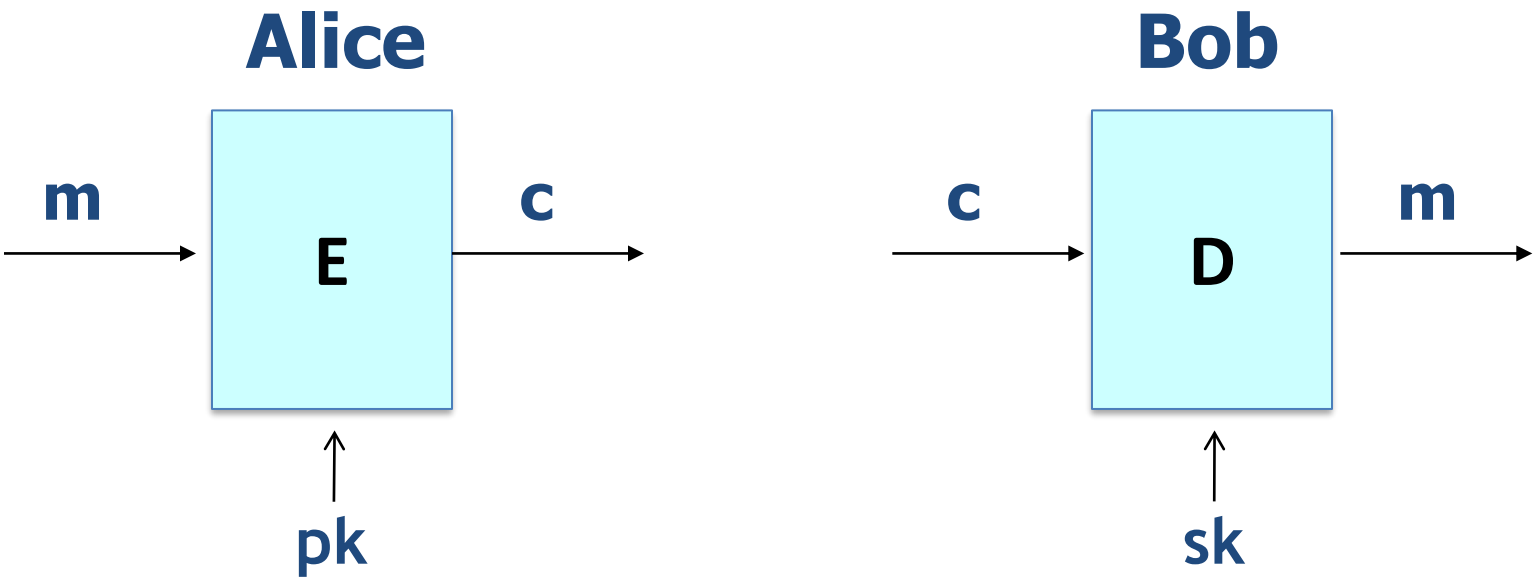
Department of Software

College of Software

Sungkyunkwan University

Public key encryption

Bob generates (pk, sk) and gives pk to Alice



Alice needs pk_{Bob} (public key management is required)

Public-key setting

- A party generates a pair of keys: a public key pk and a private key sk
  - Public key is widely disseminated
  - Private key is kept secret, and shared with no one
- Private key used by this party; public key used by everyone else
- Also called *asymmetric* cryptography

Mailbox analogy

Everyone can put a letter into this box.

But, Prof. Kim can only open this box with his private key.

Benefits of private-key crypto

- Private-key cryptography is more suitable for certain applications
  - E.g., disk encryption
- Public-key crypto is roughly 2-3 orders of magnitude slower than private-key crypto
  - If private-key crypto is an option, use it!
  - (Indeed, private-key crypto used for efficiency even in the public-key setting)

Benefits of public-key crypto

- Key distribution
  - Public keys can be distributed over public (but authenticated) channels!
- Key management in large systems of N users
  - Each user stores 1 private key and N-1 public keys; only N keys overall
  - Public keys could be stored in a central directory
- Applicability in “open systems”
  - Even parties who have no prior relationship can find others’ public keys

Trapdoor functions (TDF)

Def: a trapdoor function is a triple of efficient algorithms (G, F, F^{-1})

- $G()$: randomized algorithm outputs a key pair (pk, sk)
- $F(pk,\cdot)$: deterministic algorithm that defines a function $X \longrightarrow Y$
- $F^{-1}(sk,\cdot)$: defines a function $Y \longrightarrow X$ that inverts $F(pk,\cdot)$

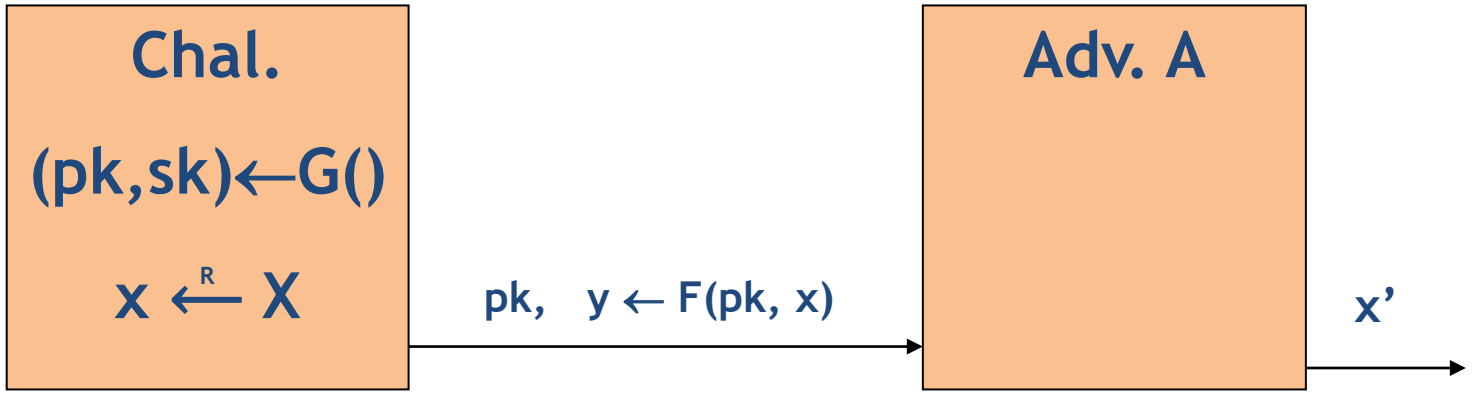
More precisely: $\forall (pk, sk)$ output by G

$$\forall x \in X: \quad F^{-1}(sk, F(pk, x)) = x$$

Secure Trapdoor Functions (TDFs)

(G, F, F^{-1}) is secure if $F(pk, \cdot)$ is an one-way function:

F can be evaluated, but cannot be inverted without sk



Def: **(G, F, F^{-1}) is a secure TDF if for all efficient A:**

Adv [A,F] = Pr[x = x'] is negligible

Construction of public key encryption

Public key encryption can be constructed from a Secure Trapdoor Function (STF).

one-way + trapdoor

(1) Easy to compute F

Anyone can encrypt a message with F.

(2) Hard to compute F^{-1}

Anyone can't decrypt the message.

(3) Easy to compute F^{-1} with secret

People who know secret can decrypt the message.

Easy to compute? Hard to compute?

Easy to compute. How? Show an *efficient* algorithm A to compute.

Which one is more difficult?

Hard to compute. How? Show no *efficient* algorithm A to compute.

How to show? NP-completeness?

This is not enough. NP-completeness is a worst-case concept. We should show that it is hard to compute on average.

A good candidate for STF

Factoring

- Given p and q, compute $n = p \cdot q$ (easy)
- Given $n = p \cdot q$, find p and q (probably hard)
  - Unfortunately, we have no idea about the trapdoor

RSA

- Given M, randomly generate n, e, d, and compute $C = M^e \pmod{n}$ such that $d \cdot e = 1 \pmod{(p-1)(q-1)}$ (easy)
- Given an RSA public key (n, e) and a ciphertext $C = M^e \pmod{n}$, compute M. (probably hard)
- Given an RSA private key (n, d) and a ciphertext $C = M^e \pmod{n}$, compute M (easy)

Factoring

- Multiplying two numbers is easy; factoring a number is hard
  - Given x, y, easy to compute x·y
  - Given x·y, hard to find x and y

- Compare:
  - Multiply 10101023 and 29100257
  - Find the factors of 293942365262911

Factoring

- It's not hard to factor *all* numbers
  - 50% of the time, random number is even
  - 1/3 of the time, random number is divisible by 3…
- The hardest numbers to factor are those that are the product of two, equal-length *primes*

The RSA problem

- The factoring problem is not *directly* useful for cryptography
  - So we will not formalize it…

- Instead, introduce a problem related to factoring: the *RSA problem*

Questions?


Sungkyunkwan
Campus
Social
Institute
Graduate
constructed
English
Professors
Building
campus
Global
Confucian
Sciences
University
Seoul
Natural
Suwon
university
School
Korean
edit
established
Humanities
lecturers
schools
Science
Administration
Academic