What is Cryptography?

Hyoungshick Kim

Department of Software

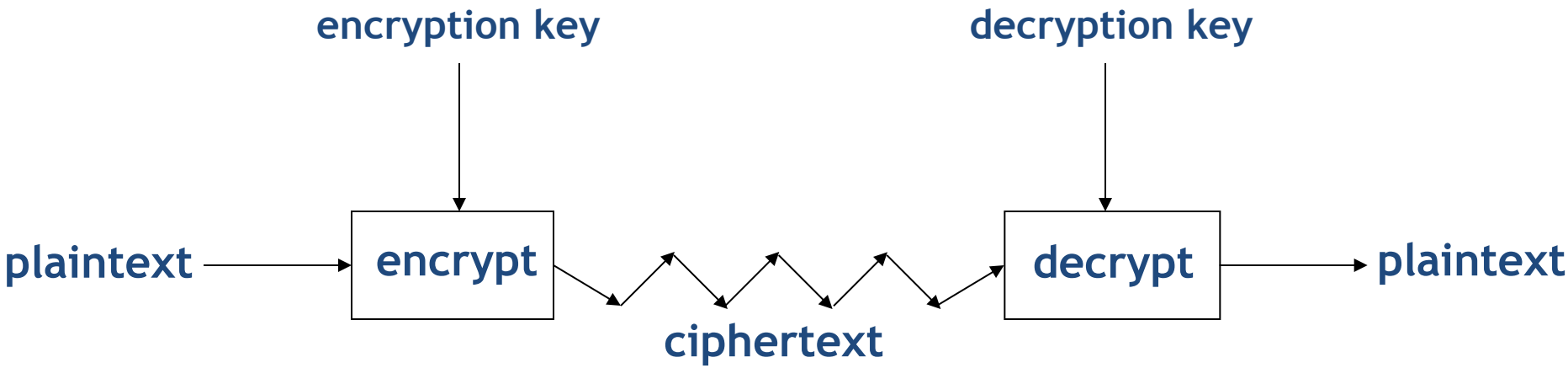
College of Software

Sungkyunkwan University

Cryptography

"secret" "writing"

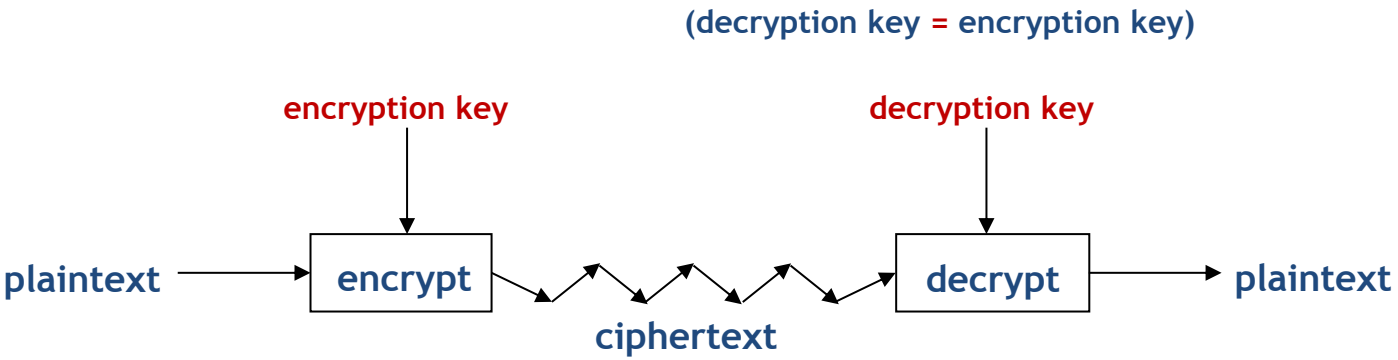
Crypto as black box



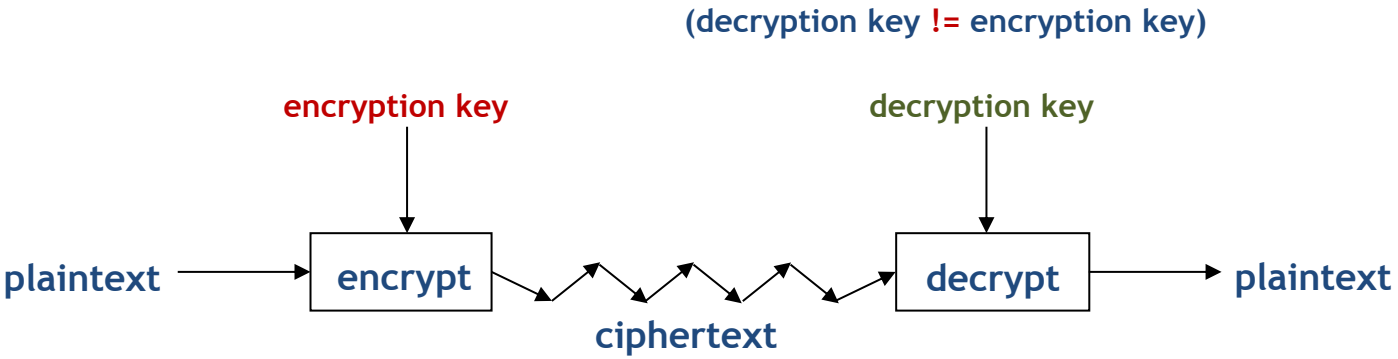
Tools for confidentiality and Integrity

Types of crypto systems

- Symmetric



- Public or Asymmetric



A framework for crypto

- Cryptography (making), cryptanalysis (breaking), cryptology (both)
- Traditional cryptanalysis – what goes wrong with the design of the algorithms
- Then – what goes wrong with their implementation (power analysis, timing attacks)
- Then – what goes wrong with their use

How to speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

Things to remember

- Cryptography is:
  - a tremendous tool
  - the basis for many security mechanisms
- Cryptography is not:
  - the solution to all security problems
  - reliable unless implemented and used properly
  - something you should try to invent yourself
    - » too many examples of broken ad-hoc designs

“If you think cryptography is the answer to your problem, you don’t know what your problem is.”

Peter G. Neumann

Three steps in cryptography

1. Precisely specify a threat (or attack) model
2. Propose a construction
3. Prove that breaking construction under the threat model will solve an underlying hard problem (security proof)

Questions?


Sungkyunkwan
Campus
Social
Graduate
Professors
English
Confucian
campus
Zone
Sciences
University
Global
Education
Seoul
Natural
Suwon
Korean
School
university
established
edit
also
Humanities
Science
schools
Administration
ASLE-Korea
Academic
Advanced
constructed
Building
Engineering
located
Joseon
Anniversary
Institute
now
two
Hall
Course
lecturers