Open Source SW Utilization

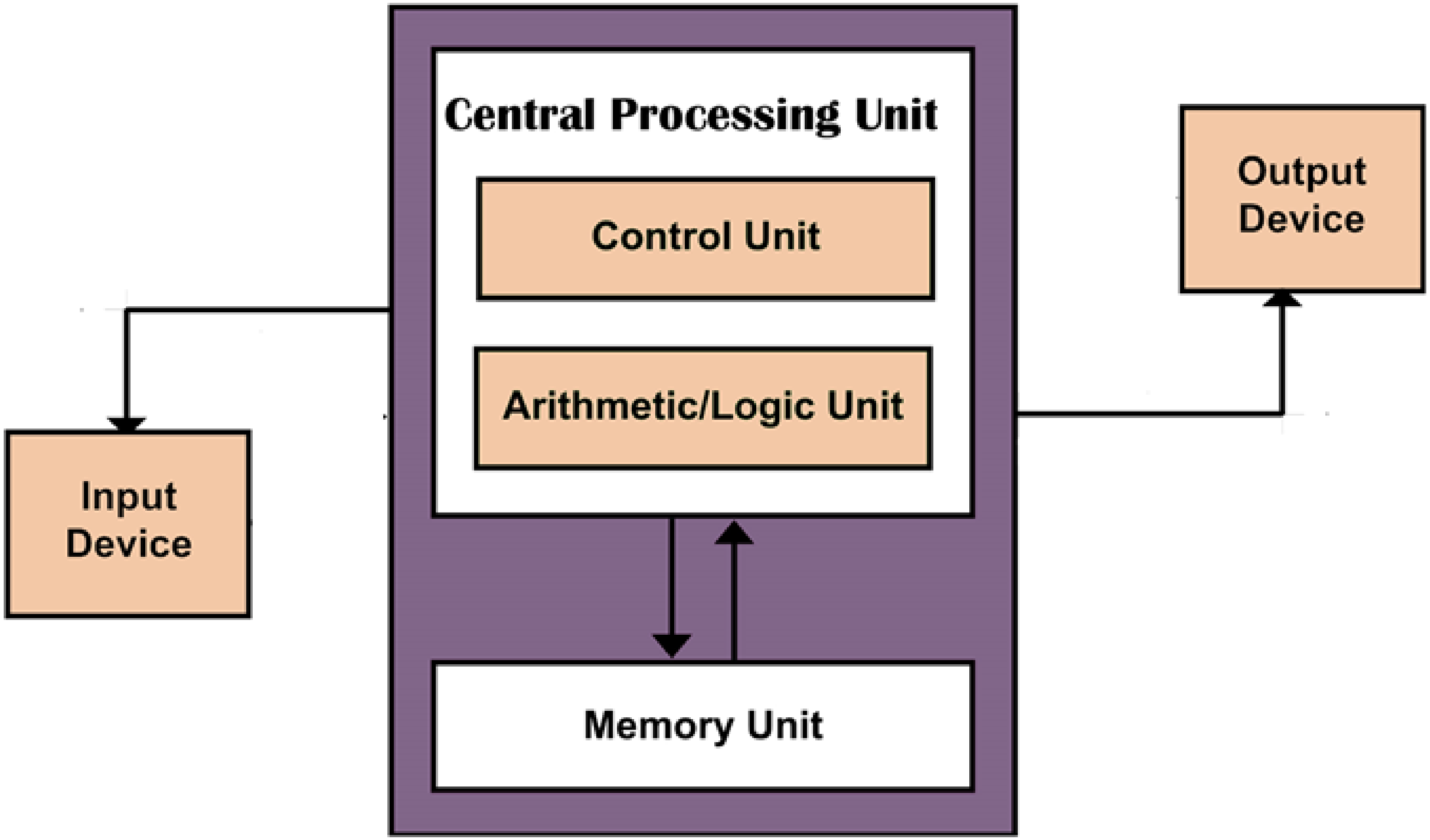
(524820-2)

송영상(Youngsang Song)

sw.yssong@dankook.ac.kr

Computer Architecture

- **Von Neumann Architecture**



Data vs. Information

Data	Information
• Raw facts	• Useful & Relevant
• Unorganized	• Organized
• Unprocessed	• Processed
• Chaotic or Unsorted	• Ordered or Sorted
• Input to a Process	• Output of a Process

01000111 11101100 10100001
00111010 01011101 00001101
...

account balance: $238,000.00

In many organizations, information/data is seen as the most valuable asset !!!

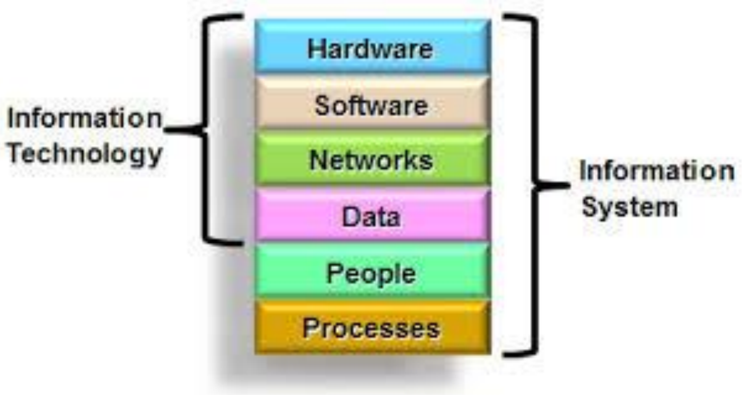
Information Technology (IT)

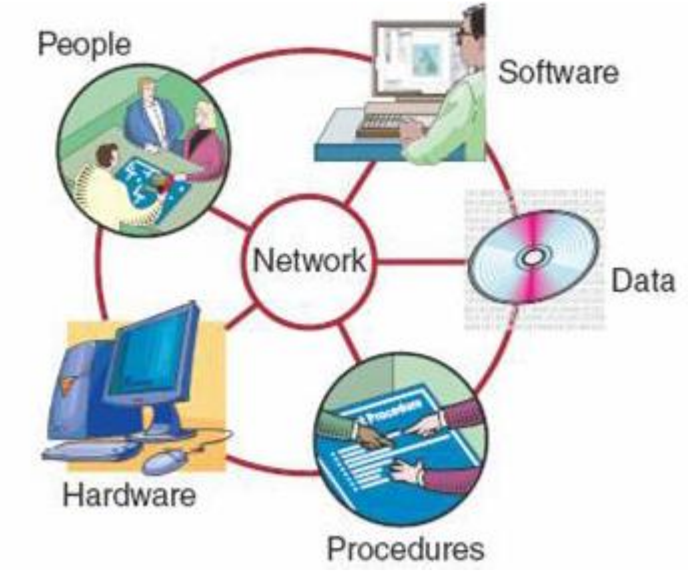
- **Information Technology** – technology involving development & use of computer systems & networks for the purpose of processing & distribution of data/information

- **Categories of IT jobs:**
  - **IT engineer -** develops new or upgrades existing IT equipment (software or hardware)
  - **IT administrator -** installs, maintains, repairs IT equip./system
  - **IT architect -** draws up plans for IT systems and how they will be implemented
  - **IT manager -** oversees other IT employees, has authority to buy technology and plan budgets
  - **IT security specialist -** creates and executes security applications to maintain system security and safety

Information System

- Entire set of data, software, hardware, networks, people, procedures and policies that deal with processing & distribution of information in an organization
  - each component has its own strengths, weaknesses, and its own security requirements





- Information is
  - stored on computer H/W,
  - manipulated by S/W,
  - Transmitted by communication,
  - used by people
  - controlled by policies

What is Security?

- Security = State of being secure, free from danger (threat/risk/vulnerability)
- Security is to enforce a desired property *in the presence of an attacker*
  - Data confidentiality
  - Data and computation integrity
  - Availability
  - Authentication (Authenticity)
  - User privacy (Anonymity)
  - …
- Information Security – practice of defending information from unauthorized
  - Access (read, write, append)
  - Use
  - Recording
  - Disruption (분열, 혼란, 중단, 붕괴) – DoS (Denial-of-Service)
  - Destruction (Deletion) – DoS
  - Modification (Alternation, Tampering)
  - …

What is Computer Security?

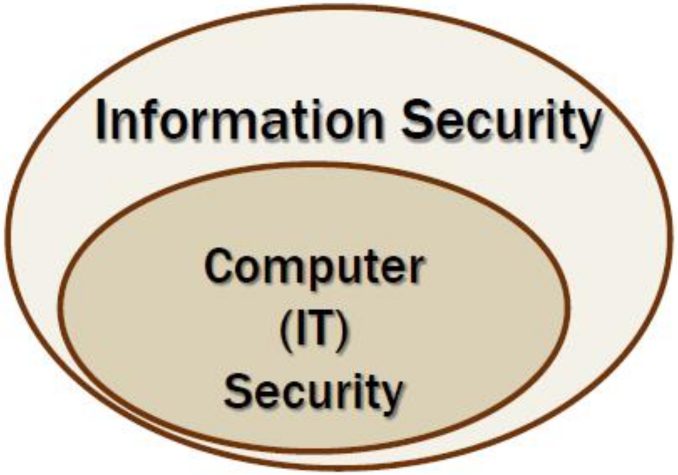
- Computer security is the protection of computer systems against adversarial environments
  - allow intended use
  - prevent unintended use

- Computer Security is the protection of computing systems and the data that they store or access

- We will try to understand:
  - why computer systems are insecure
  - how to build secure systems

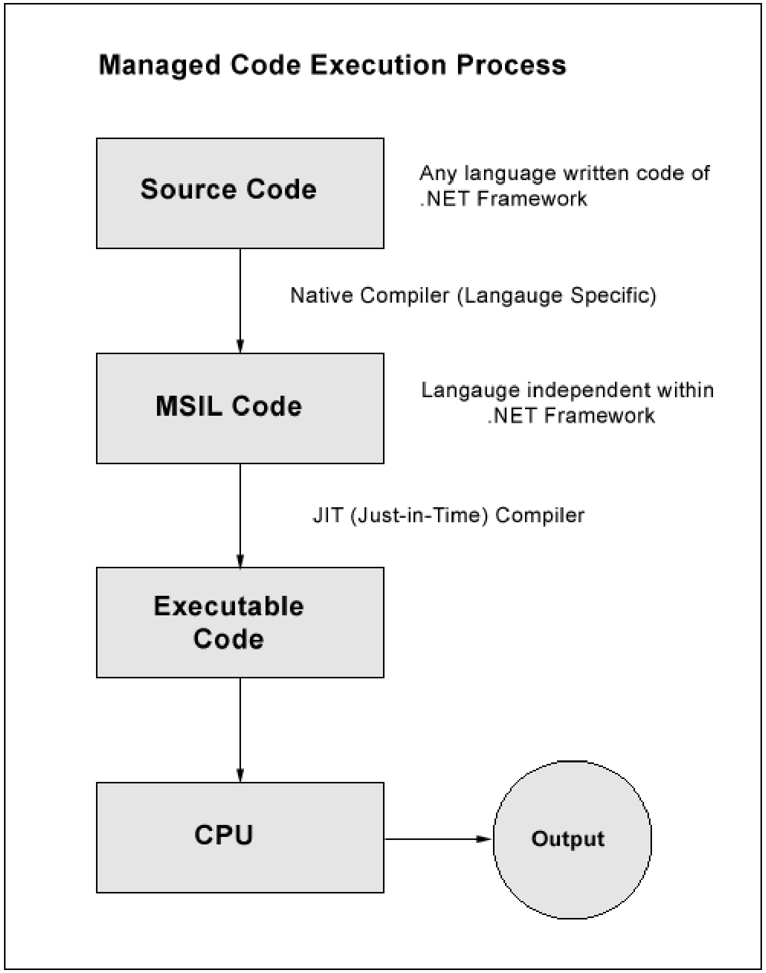
Computer Security vs. Information Security

- **Computer security** (aka IT security) is mostly concerned with information in ‘digital form’
- **Information security** is concerned with information in any form it may take: electronic, print, etc.



Execution Process

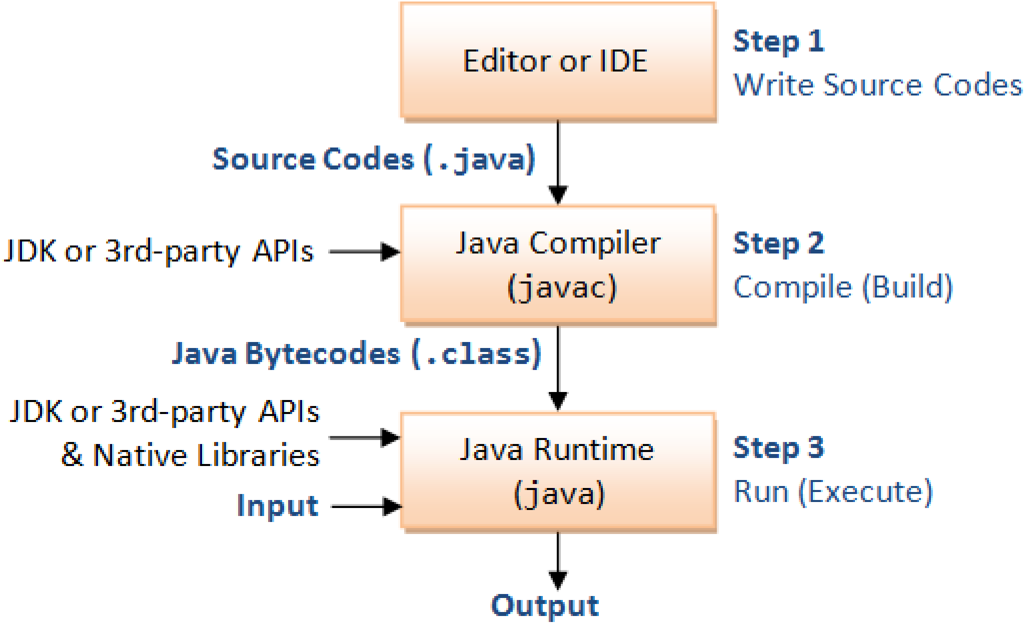
- .Net



Managed Code Execution Process
Source Code
Any language written code of .NET Framework
Native Compiler (Langauge Specific)
MSIL Code
Langauge independent within .NET Framework
JIT (Just-in-Time) Compiler
Executable Code
CPU
Output

MSIL(Microsoft Intermediate Language)

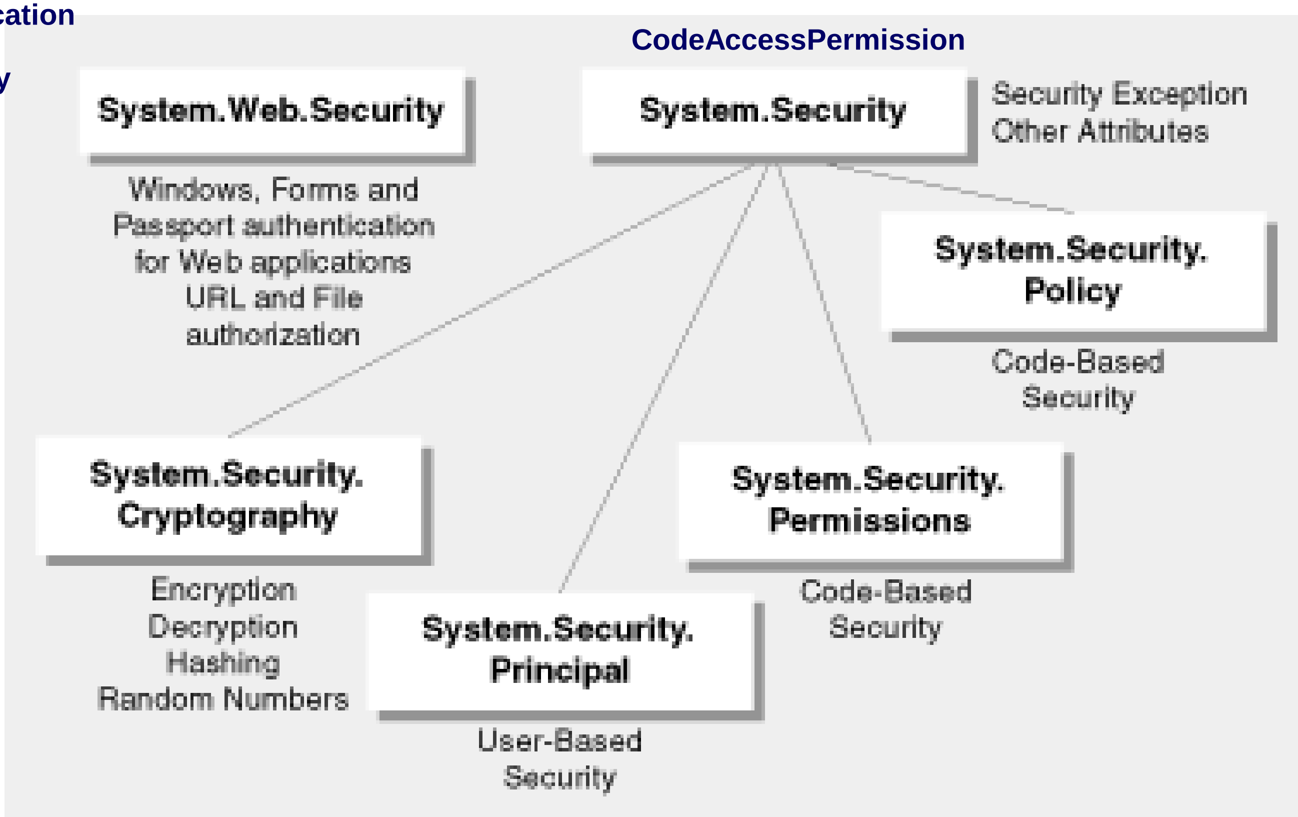
- Java



Microsoft security policy

Microsoft .Net security namespaces

Url and File AuthorizationModule
- **FormsAuthentication**
- **FormsIdentity**
- **PassportIdentity**

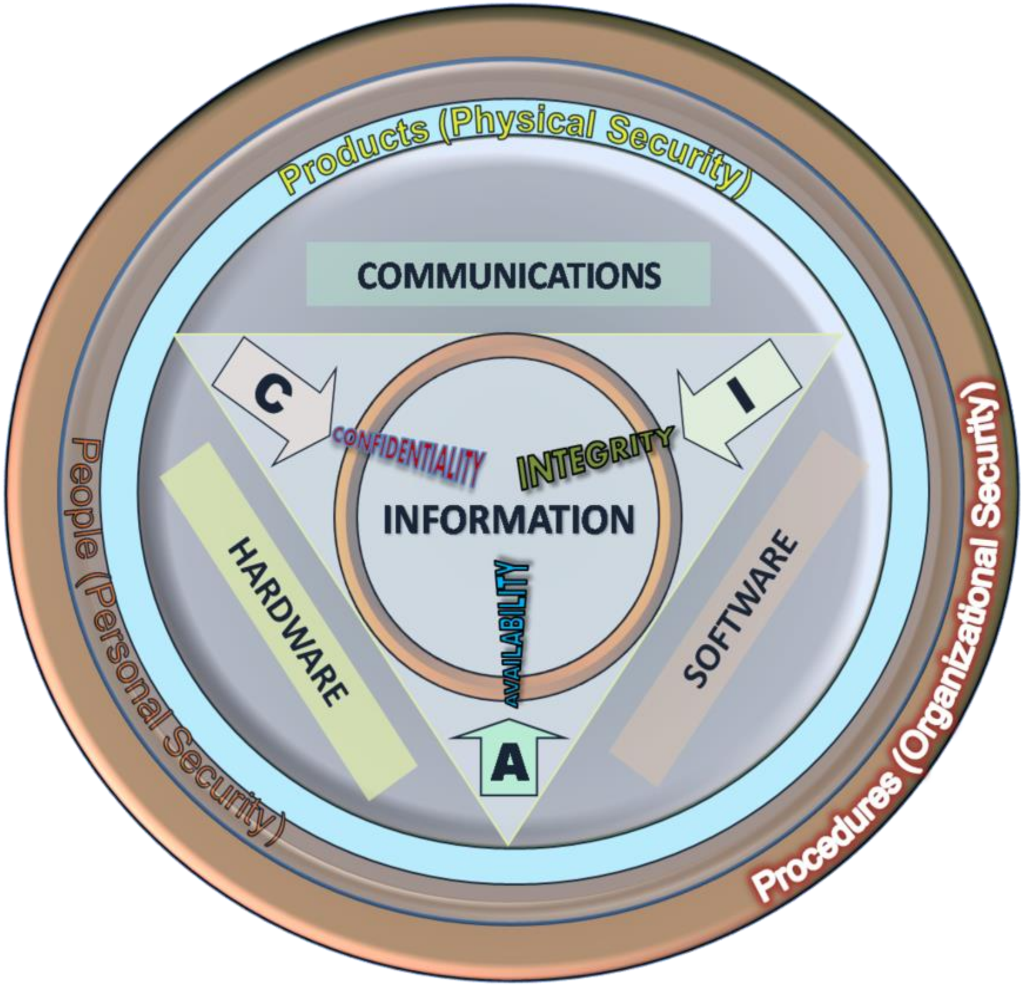


CodeAccessPermission

Reference : https://msdn.microsoft.com/en-us/library/ff648652.aspx

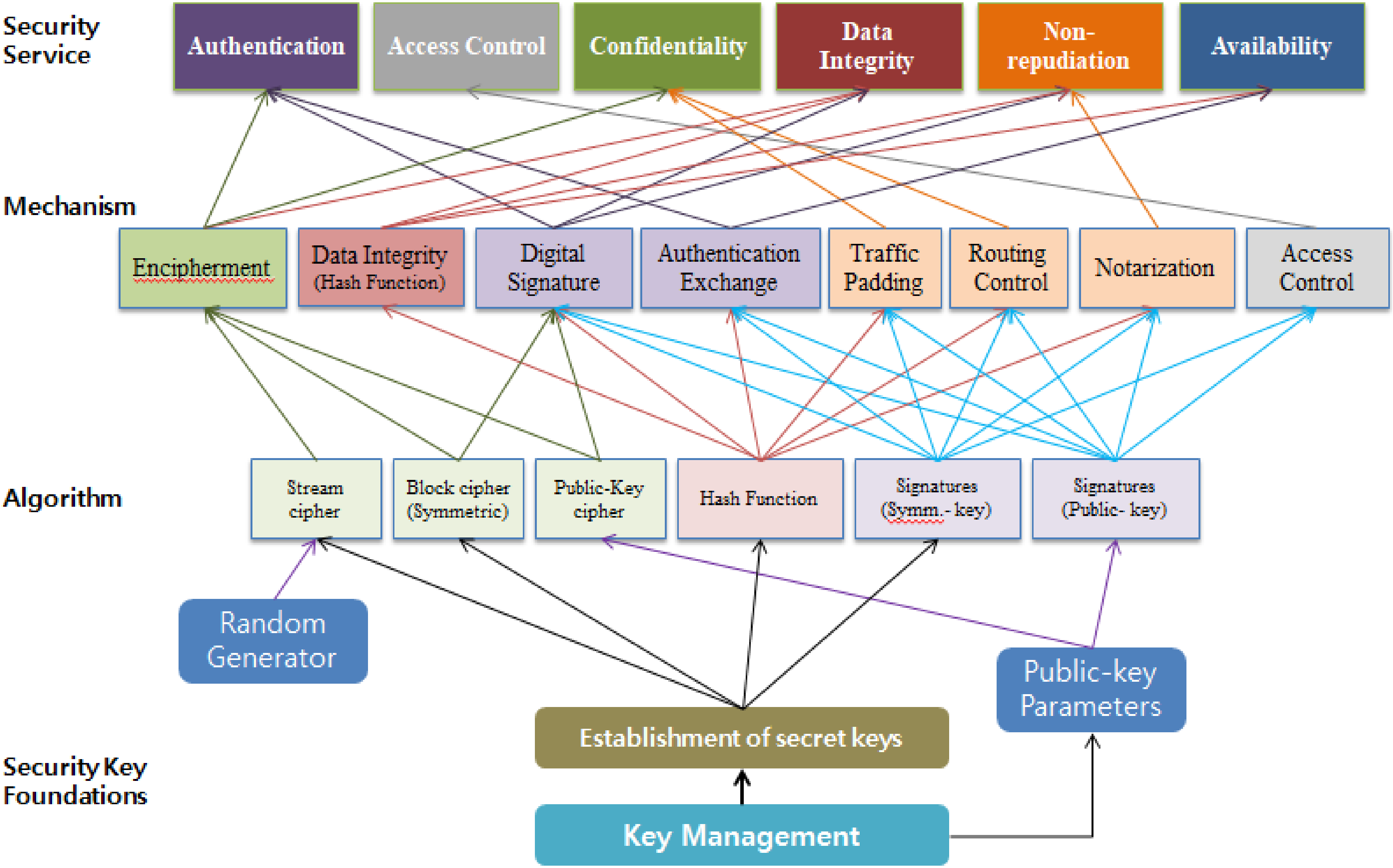
Information Security

- Information security attributes(CIA)
  - Confidentiality
  - Integrity
  - Availability


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

https://en.wikipedia.org/wiki/Information_security

Whole Layer of Security



Crypto

- **Cryptology** — The art and science of making and breaking "secret codes"

  = Crypto (Hidden) + Logos(Word)

  = Cryptography + Cryptanalysis

- **Cryptography** — making "secret codes"
- **Cryptanalysis** — breaking "secret codes"
- **Crypto** — all of the above (and more)

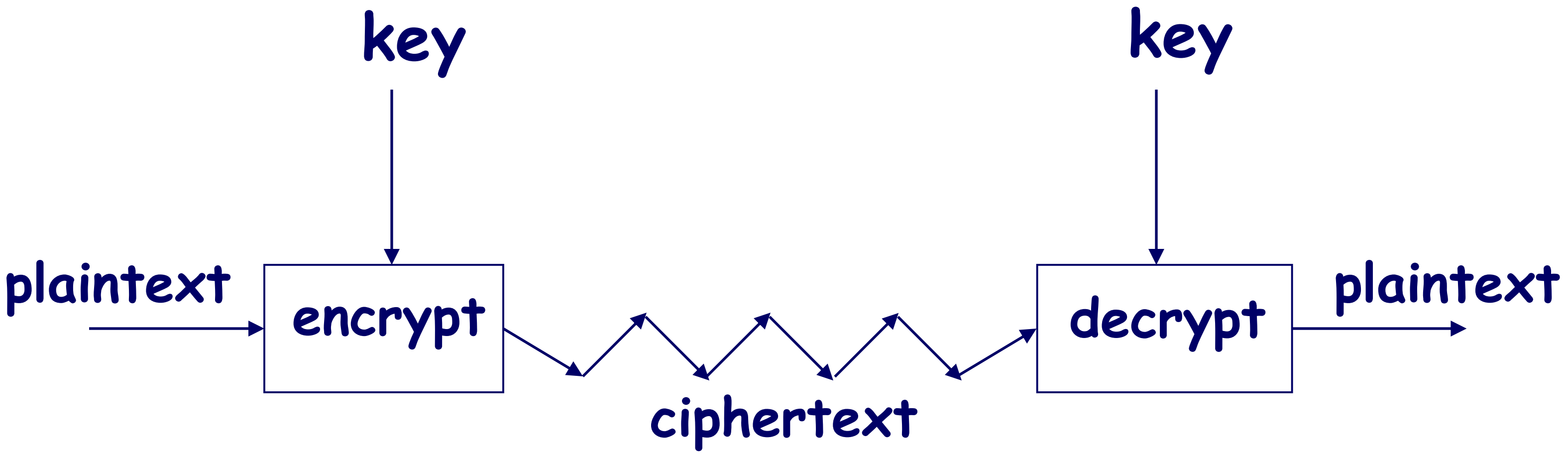
- **Cryptographic algorithm = cipher**

Cryptography

암호관련 용어

- Plaintext(Message, 평문) : 전달할 원문
- Ciphertext(암호문) : 암호화한 문서
- Encryption (Encipher, 암호화) : 원문을 위장하는 것
- Decryption (Decipher, 복호화) : 암호문을 원문으로 복구하는 것
- Cryptography : 전달할 내용의 보안을 연구하는 학문
- Cryptographer : Cryptography를 수행하는 사람
- Cryptanalysis : 암호문의 해독을 연구하는 학문
- Cryptology : Cryptography와 Cryptanalysis를 포함하는 수학의 한 분야
- Cryptologist : Cryptology를 연구하는 사람
- Cryptographic : Algorithm 암호화와 복호화를 위해 사용하는 함수

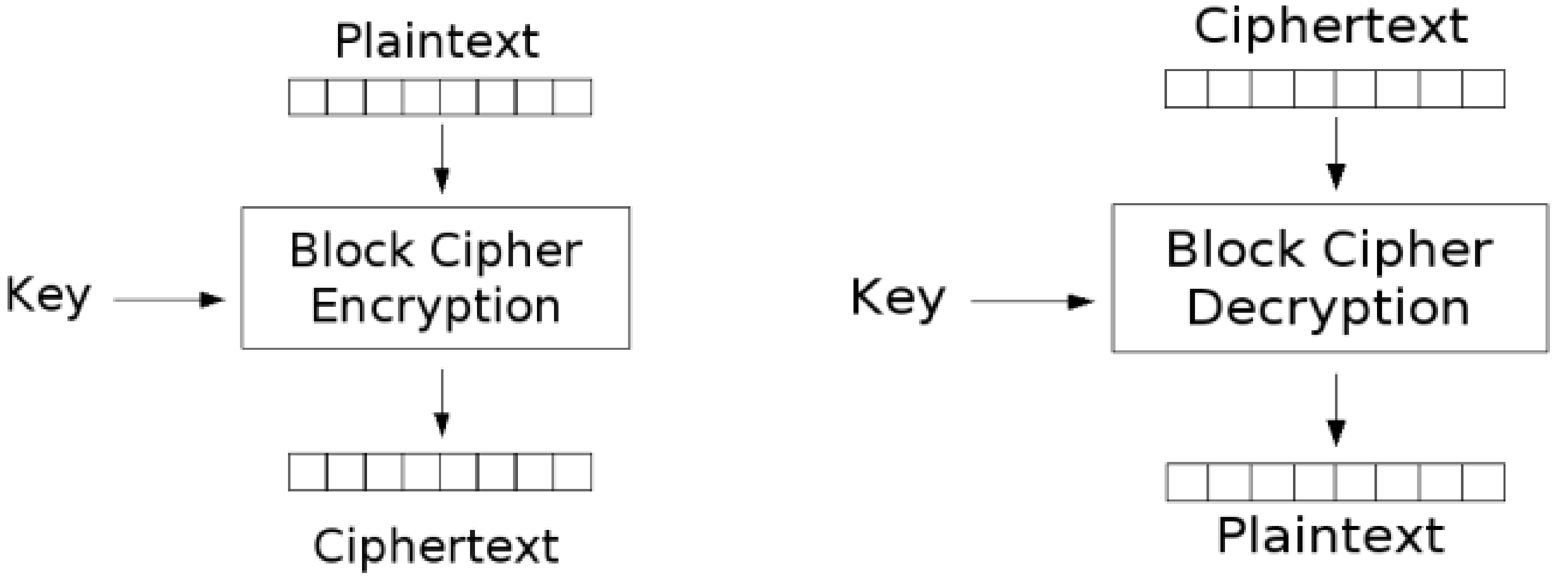
Crypto as Black Box



A generic use of crypto

Symmetric Key Crypto

- Block cipher — based on codebook concept
  - Block cipher key determines a "electronic" codebook
  - Each key yields a different codebook
  - Employ both "confusion" and "diffusion"



Symmetric Key Crypto

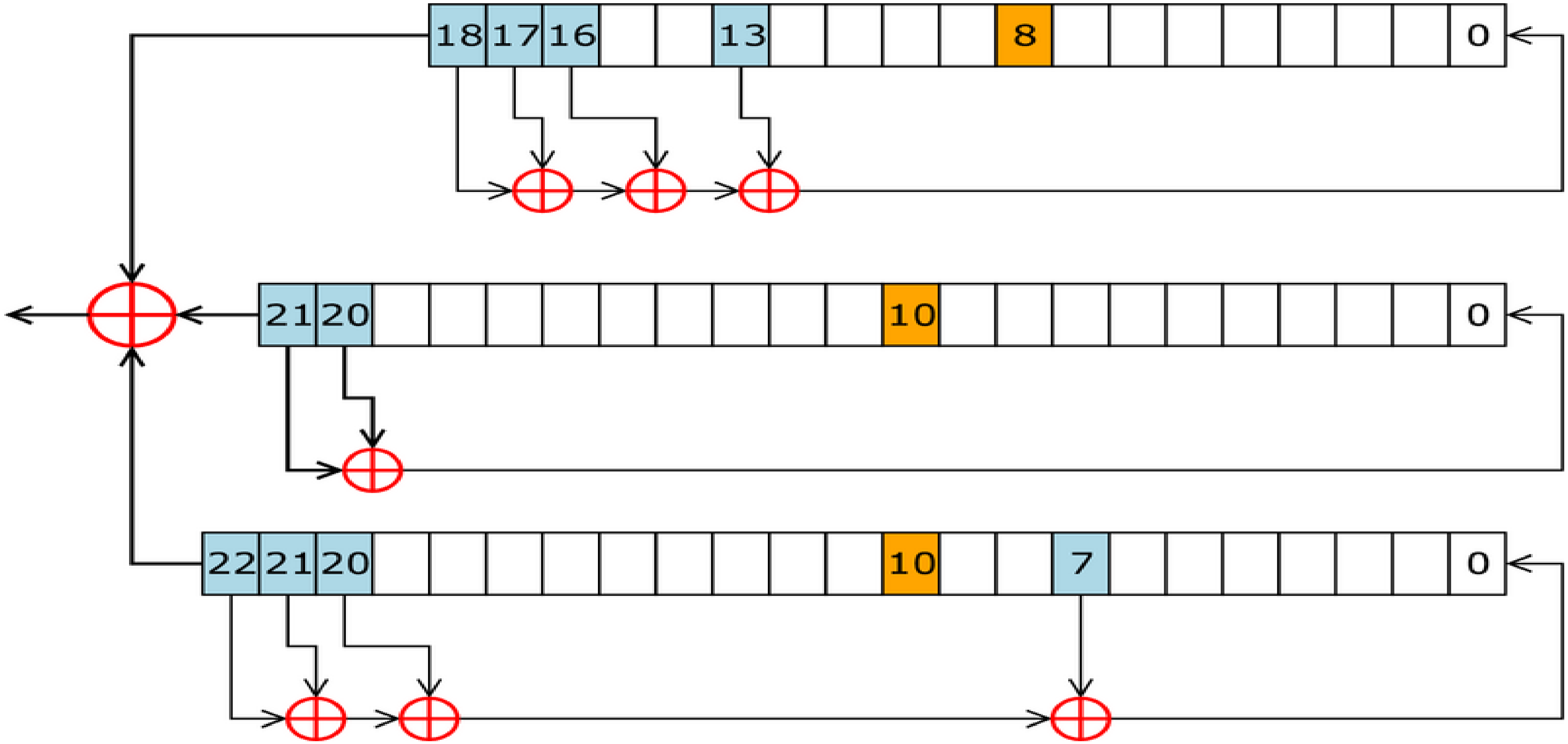
- Examples of Block cipher
  - Data Encryption Stantard(DES): relatively simple,
  - Advanced Encryption STD(AES)
  - International Data Encrytption Alg.(IEDA)
  - Blowfish, RC6
  - Tiny Encryption Algorithm
- Mode of Operation of block cipher
  - Examples of block cipher mode Op
    - Electronic codebook (EOB)
    - Cipher-block chaining (CBC)
    - Cipher feedback (CFB)
    - Output feedback (OFB)
    - Counter (CTR)
- Data integrity of block cipher
  - Message Authentication code (MAC)

Stream Ciphers

Stream Ciphers

- Not as popular today as block ciphers
- Key K of n bits stretches it into a long keystream
- Function of stream cipher
  - StreamCipher(K) = S where K:key, S:keystream
  - S is used like a one-time pad
    - $c_0 = p_0 \oplus s_0$, $c_1 = p_1 \oplus s_1$, $c_2 = p_2 \oplus s_2$, …
    - $p_0 = c_0 \oplus s_0$, $p_1 = c_1 \oplus s_1$, $p_2 = c_2 \oplus s_2$, …
- Sender and receiver have same stream cipher algorithm and both know the key K

A5/1



- Each value is a single bit
- Key is used as initial fill of registers
- Each register steps or not, based on (x_8, y_{10}, z_{10})
- Keystream bit is XOR of right bits of registers

Block Ciphers

Feistel 구조

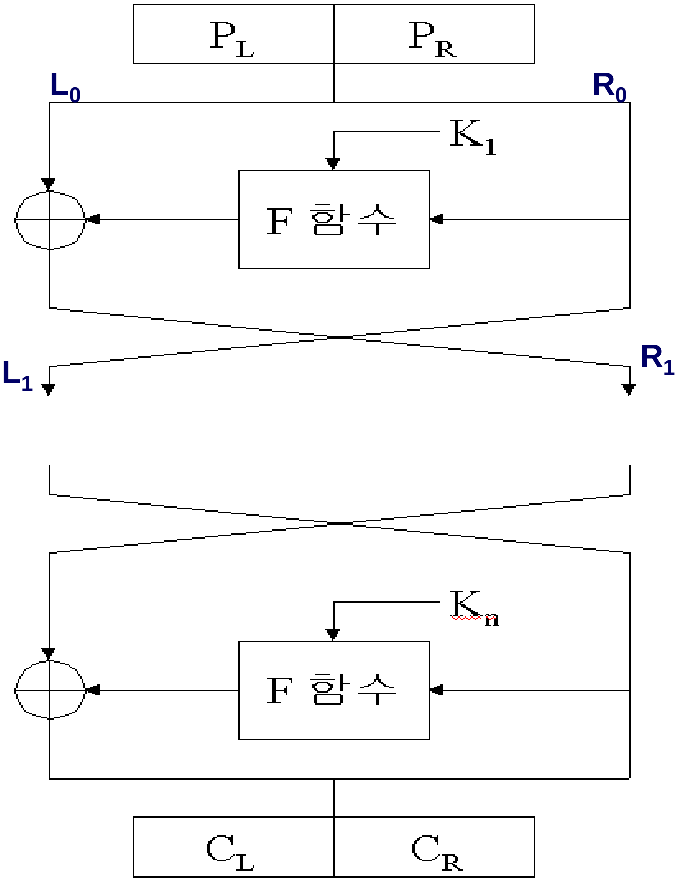
- Feistel 구조는 블록 암호를 만들 때 가장 많이 사용되는 구조이다.
- Definition

  Plaintext(P_L, P_R)

  $L_i = R_{i-1}$,
  $R_i = L_{i-1}$ xor $f_{Ki}(R_{i-1}, K_i)$

  Ciphertext(C_L, C_R) :

  (Lr, Rr) r : round 수
- 1975년 NDS(New Deal Standard)
  → 1977년 암호 해독



특 징

- N-bit의 평문을 N-bit의 암호문으로 바꾸는 알고리즘이다.
- DES 알고리즘
  - Confusion(substitution)

    어떤 비트들의 유형을 다른 비트들로 전환함으로써 혼돈성질을 제공
  - Diffusion(permutation)

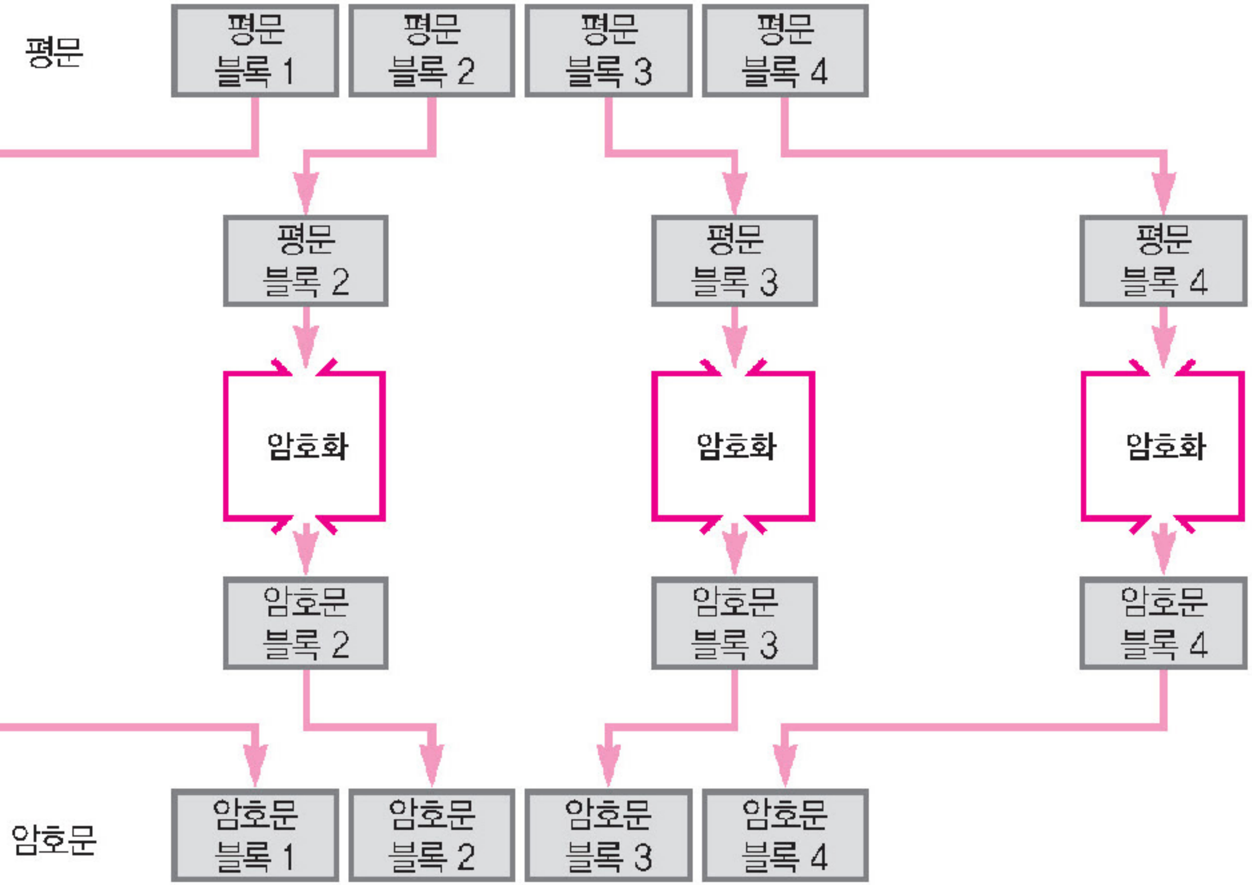
    비트들의 순서를 재배열함으로써 확산의 효과를 띰

4. 운용 모드

- DES를 비롯한 블록암호에 사용하는 목적에 따라 다양한 운용모드에 의해 운용된다.
- EBC
- CBC
- CFB
- OFB

ECB(Electronic CodeBook Mode)

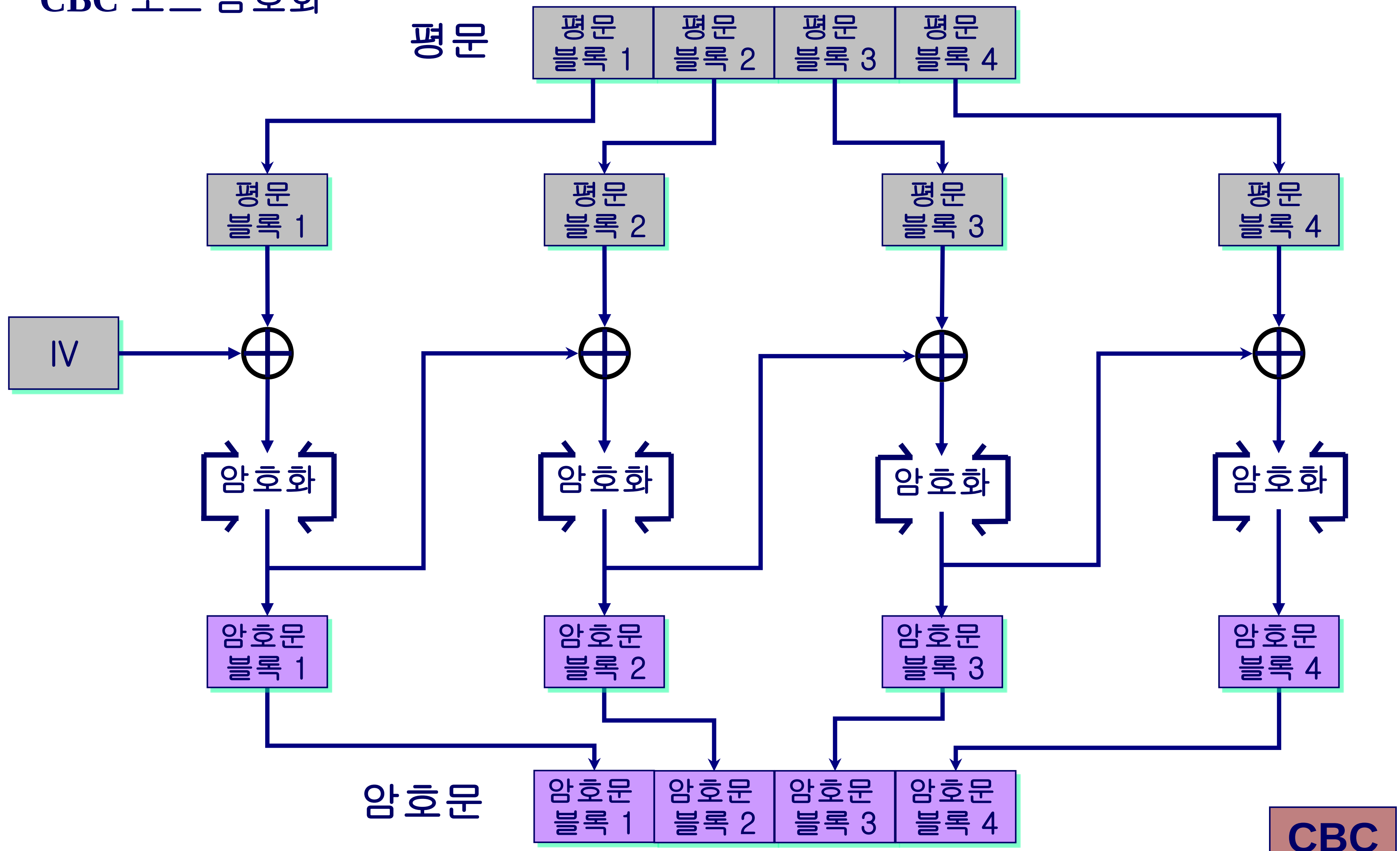
(a) ECB 모드에 의한 암호화



ECB

CBC(Cipher Block Chaining Mode)

CBC 모드 암호화

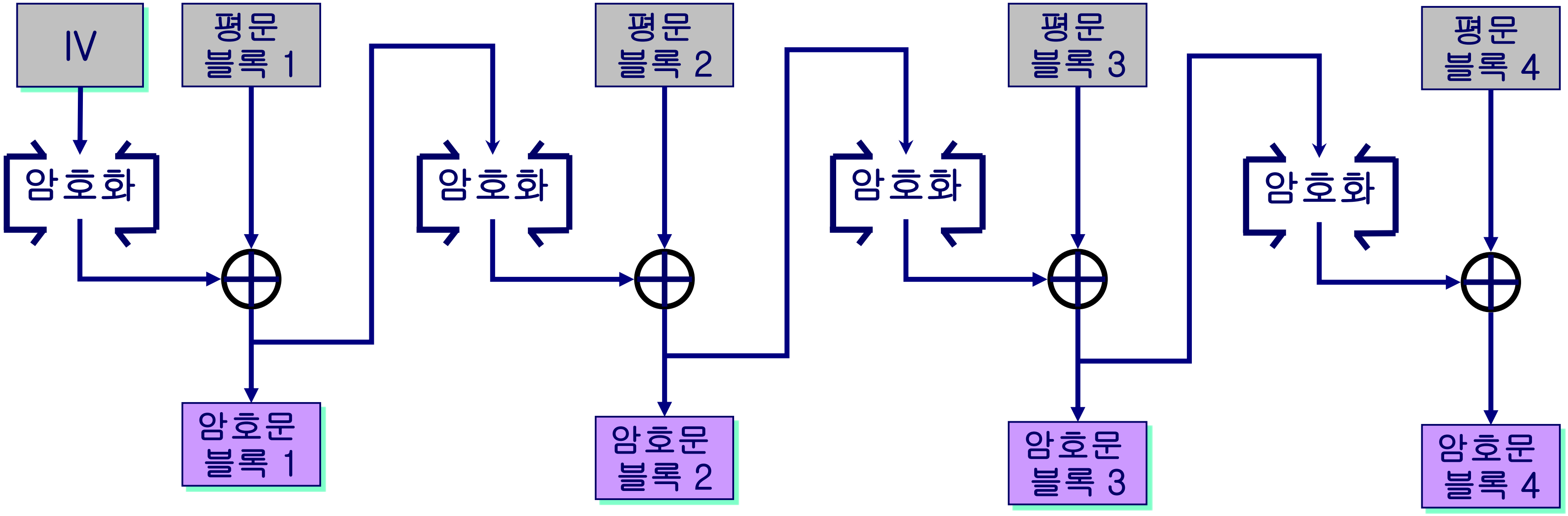


CBC

CFB(Cipher FeedBack Mode)

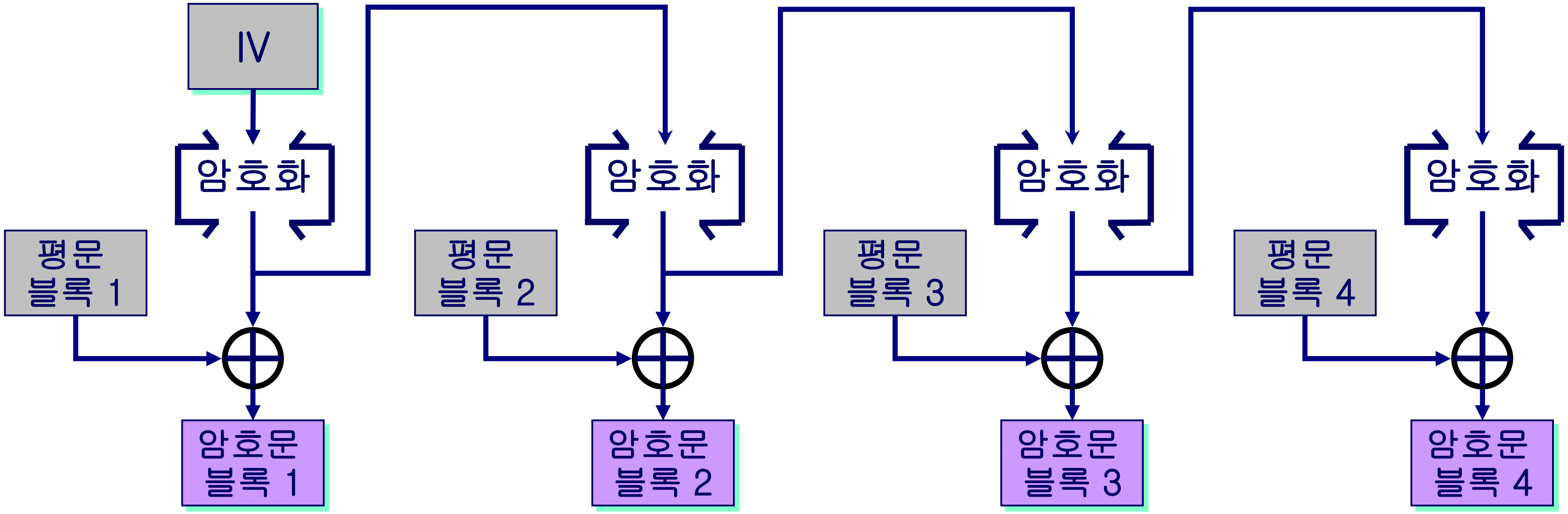
- 현재의 암호문이 다음 암호문에도 영향을 미친다.
- 오류의 파급효과가 지속된다.

CFB 모드 암호화



OFB(Output FeedBack Mode)

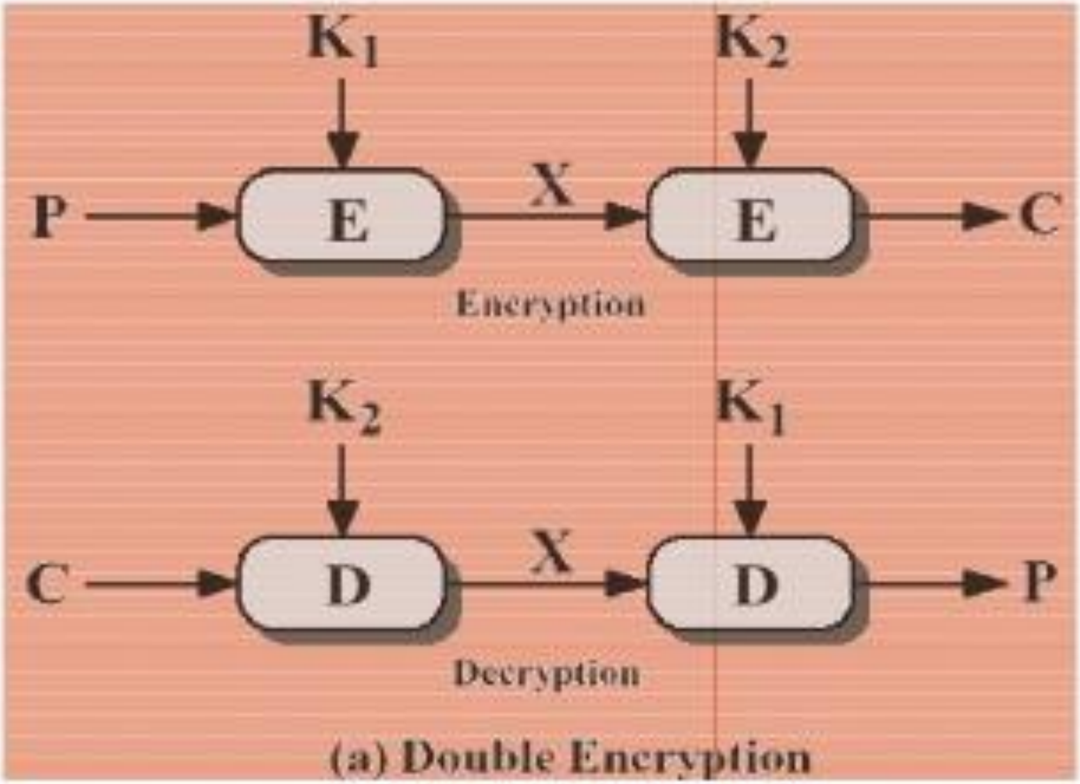
OFB 모드 암호화



OFB

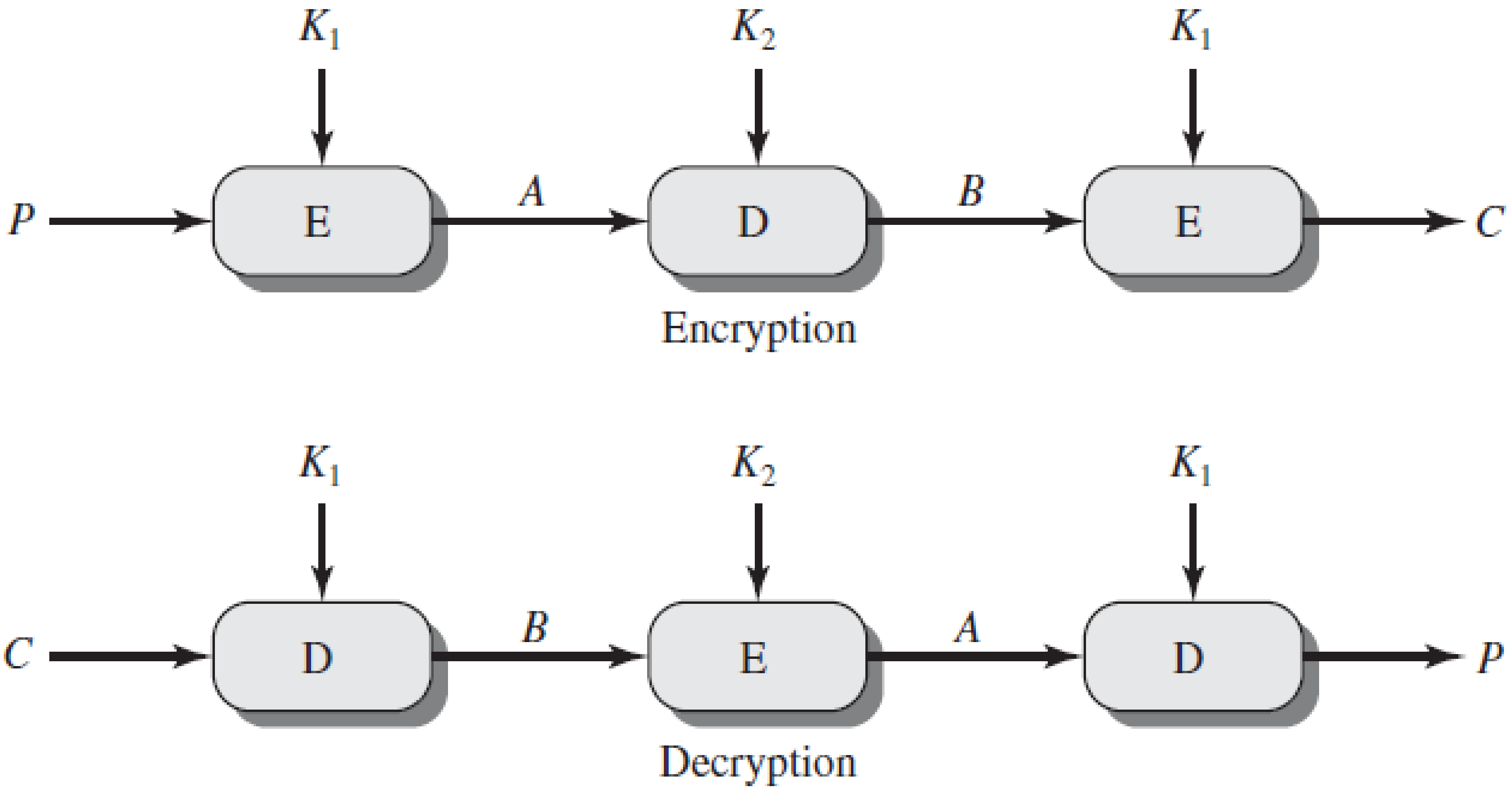
Double DES

- Key size $K=(K_1, K_2)$: 112 bits
- $C=E_{K2}(E_{K1}(P))$



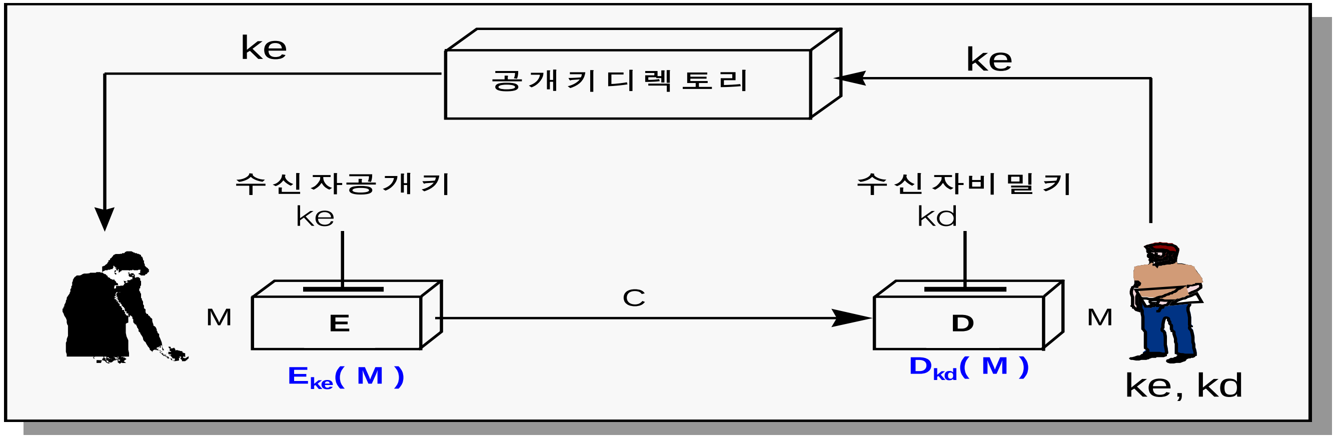
(a) Double Encryption

Triple DES



Public key Ciphers

공개키 암호 시스템의 원리.

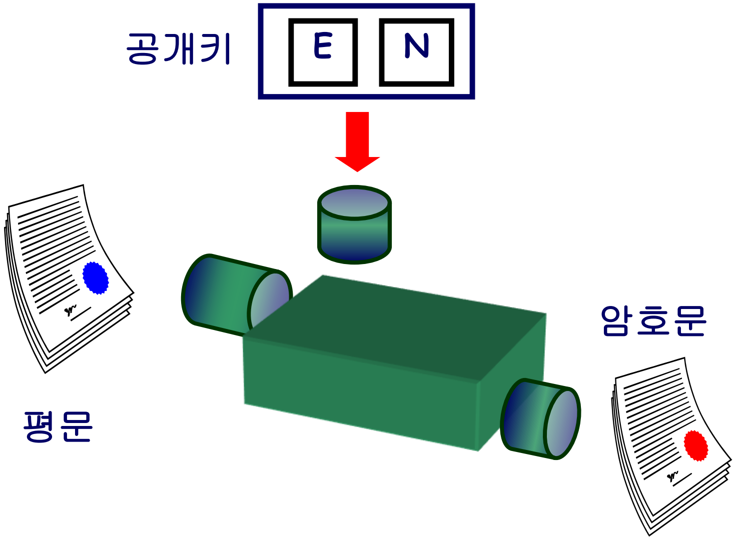


Ke : 공개키, Kd : 비밀키.

M : Message, C : Ciphertext.

E : Encryption, D : Decryption.

RSA의 암호화와 복호화



공개키

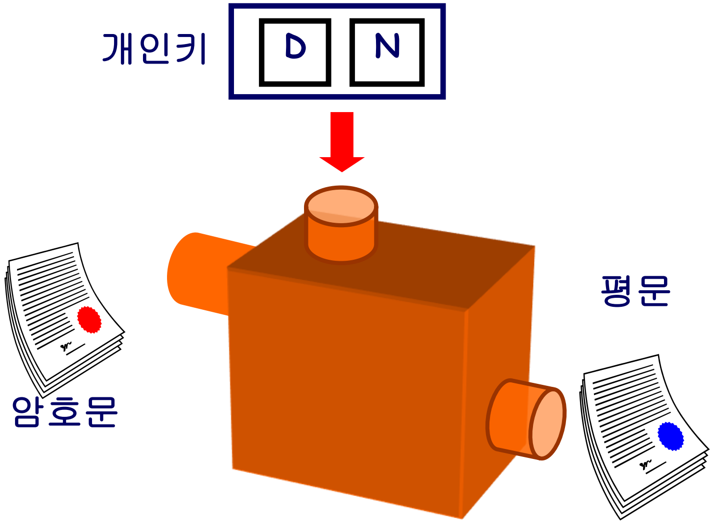
E N

평문

암호문

RSA 암호화

암호문=평문^{E} mod N



개인키

D N

암호문

평문

RSA 복호화

평=암호문^{D} mod N

암호화 및 복호화.

암호와 복호화는 평문블럭 M과 암호문 블록 **C**에 대하여 다음의 형태를 따른다.

암호화 : $\mathbf{C} = \mathbf{M}^e \bmod n$.

복호화 : $M = \mathbf{C}^d \bmod n$.

C : Ciphertext, M : Message.

e : 암호(공개)키, d : 복호(비밀)키.

키 생성 알고리즘

◎ 두 솟수 p, q 선택.

◎ $n = p \bullet q$ 계산.

◎ $\O(n) = (p - 1) \bullet (q - 1)$ 계산.

◎ $\O(n)$과 서로소이고, $1 < d < \O(n)$을 만족하는 d 선택.

◎ $d \bullet e = 1 \bmod \O(n)$에서 e를 구한다.

※ 공개키 = $\{e, n\}$, 비밀키 = $\{d, n\}$

암호화 및 복호화.

① 두 솟수 $p = 7$, $q = 17$ 선택.

② $n = p \bullet q = 7 \bullet 17 = 119$ 계산.

③ Ø(n) = (p - 1) • (q - 1) = 6 • 16 = 96 계산.

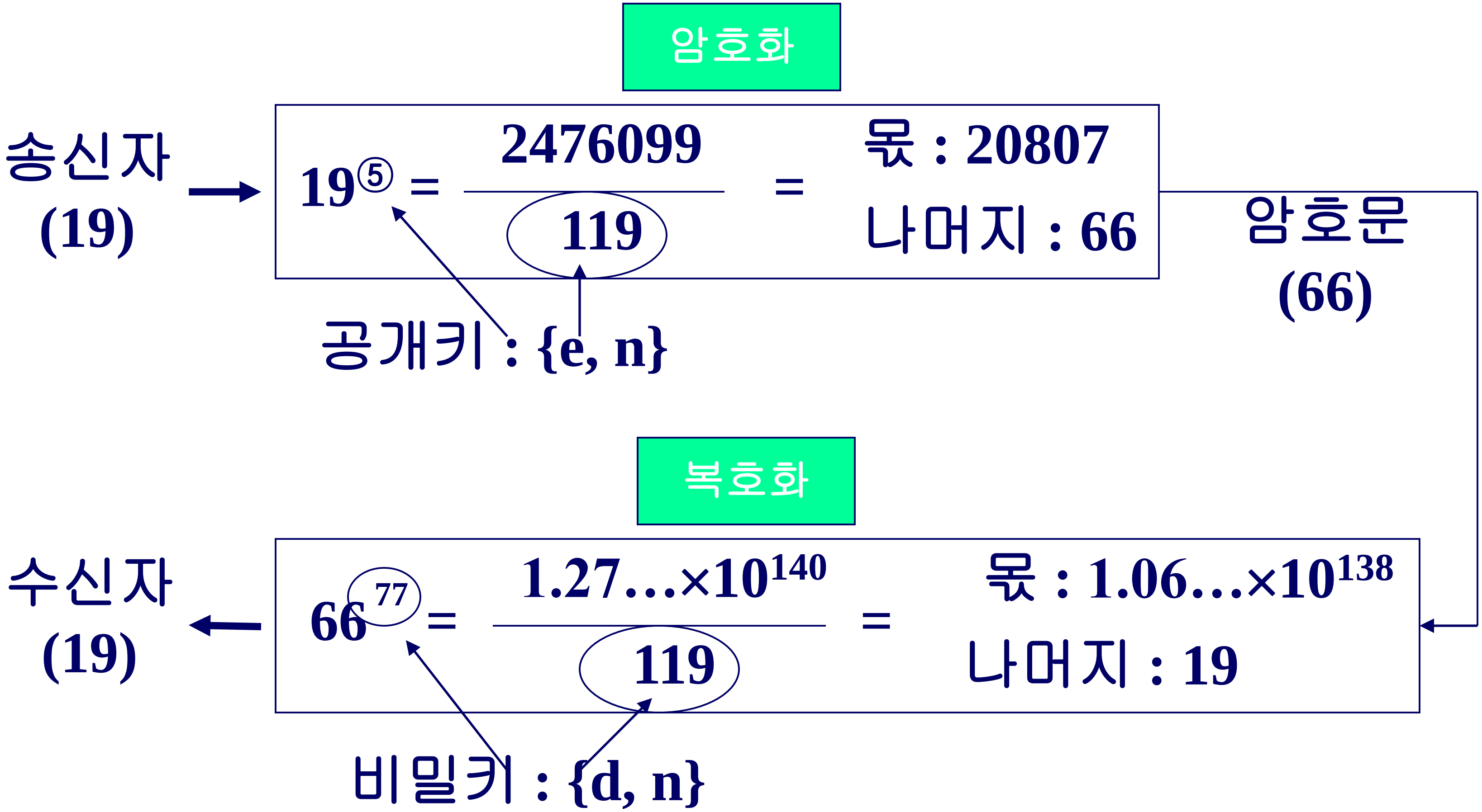
④ Ø(n) = 96과 서로소이고, 1 < e < Ø(n)인 e선택.

e = 5. (임의 선택)

⑤ $d \bullet e = 1 \bmod 96$에서 d 결정.

d = 77. (Euclid 호제법)

암호화 및 복호화.



암호화

송신자
(19)

$$19^{5} = \frac{2476099}{119} =$$

몫 : 20807

나머지 : 66

암호문
(66)

공개키 : {e, n}

복호화

수신자
(19)

$$66^{77} = \frac{1.27\ldots\times10^{140}}{119} =$$

몫 : $1.06\ldots\times10^{138}$

나머지 : 19

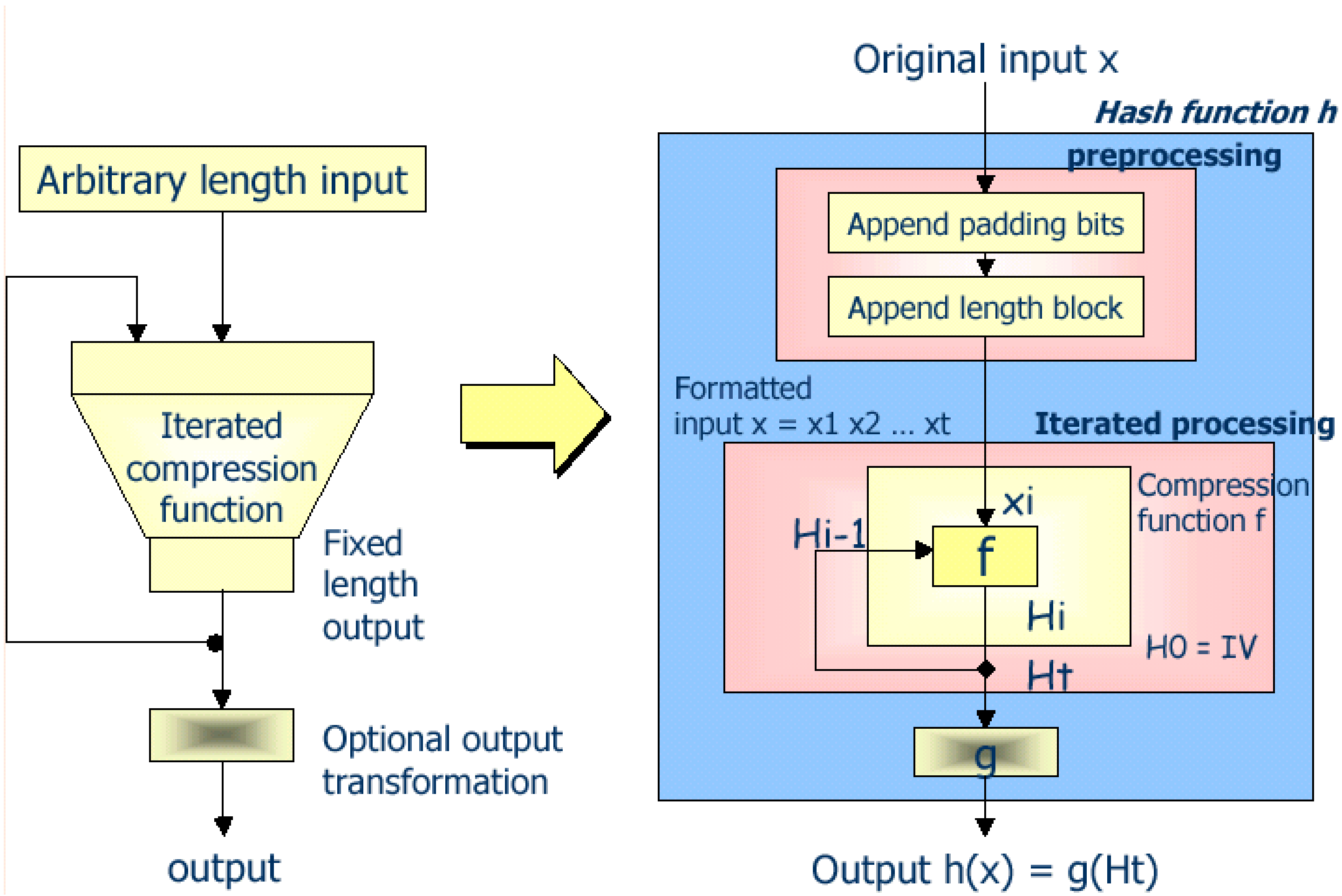
비밀키 : {d, n}

다른 공개 키 암호

- **RSA**는 현재 가장 많이 보급되어 있는 공개 키 암호 알고리즘이다
- **RSA** 이외에도 공개 키 암호는 많이 있다.
  - **ElGamal** 방식
  - **Rabin** 방식
  - 타원 곡선 암호
- 이들 암호는 모두 암호와 디지털 서명에 이용할 수 있다.

Hash Function

General Model for Iterated Hash Function



Arbitrary length input

Iterated compression function

Fixed length output

Optional output transformation

output

Original input x

Hash function h

preprocessing

Append padding bits

Append length block

Formatted input x = x1 x2 ... xt

Iterated processing

Compression function f

xi

Hi-1

f

Hi

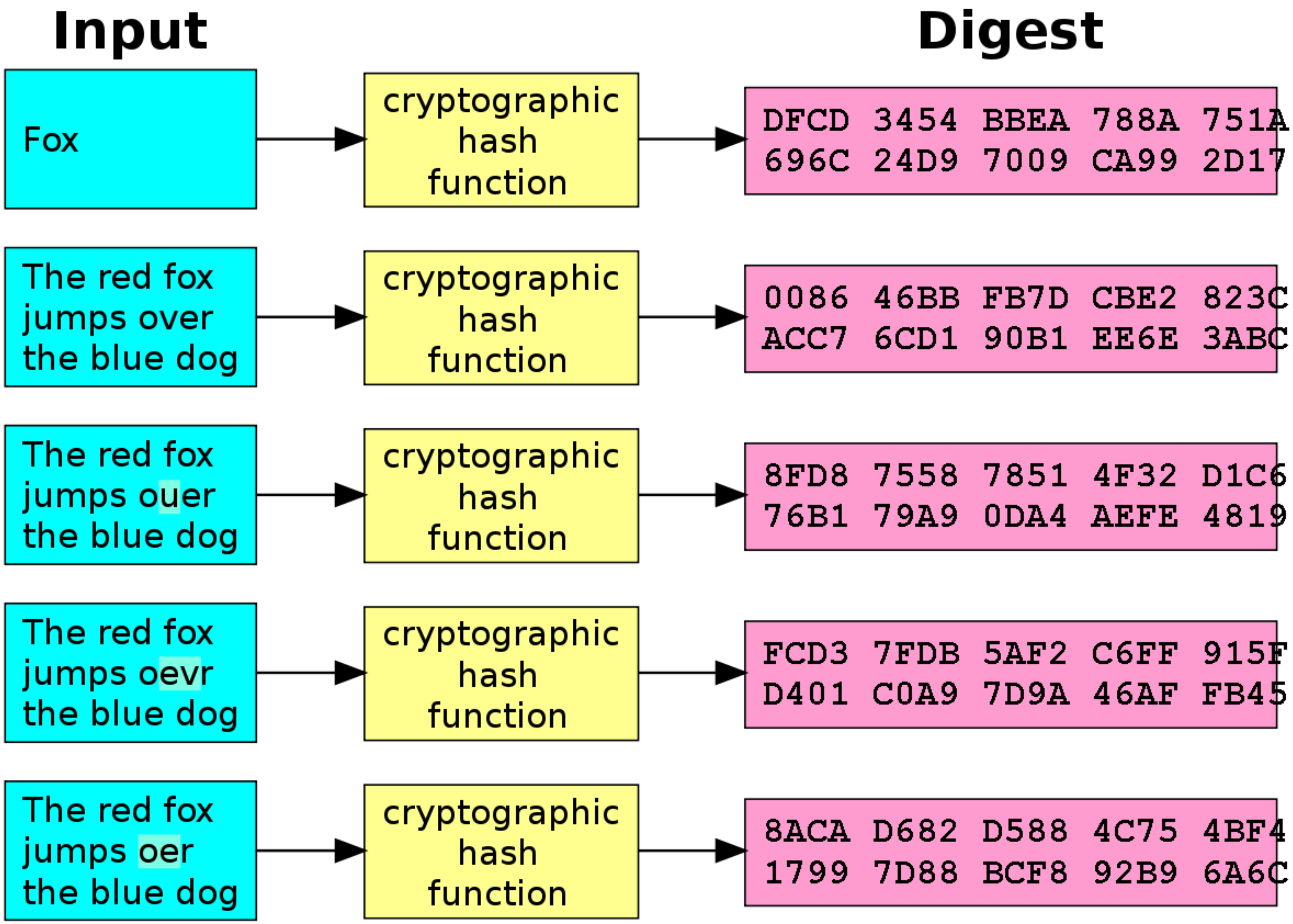
H0 = IV

Ht

g

Output h(x) = g(Ht)

General Model for Iterated Hash Function



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

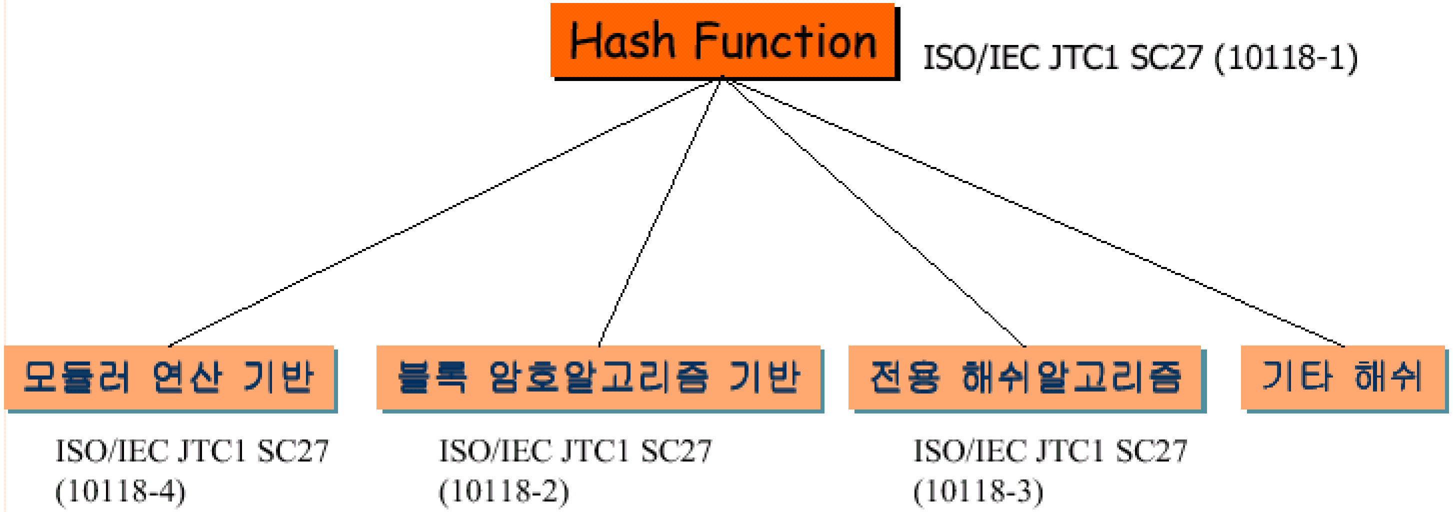
The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

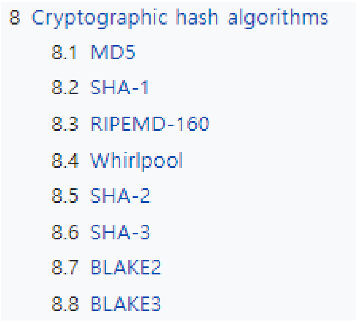
Unkeyed Hash Function (MDCs)

- 기반논리별 분류


Hash Function
ISO/IEC JTC1 SC27 (10118-1)
모듈러 연산 기반
블록 암호알고리즘 기반
전용 해쉬알고리즘
기타 해쉬
ISO/IEC JTC1 SC27 (10118-4)
ISO/IEC JTC1 SC27 (10118-2)
ISO/IEC JTC1 SC27 (10118-3)

MASH-1
MASH-2

SHA-1
MD2, MD4, MD5,
RIPEMD
HAVAL



8 Cryptographic hash algorithms
8.1 MD5
8.2 SHA-1
8.3 RIPEMD-160
8.4 Whirlpool
8.5 SHA-2
8.6 SHA-3
8.7 BLAKE2
8.8 BLAKE3

Reference

- https://en.wikipedia.org/wiki/Cryptographic_hash_function
- https://cryptography.io/en/latest/hazmat/primitives/symmetric-encryption/#module-cryptography.hazmat.primitives.ciphers.modes
- https://www.ibm.com/kr-ko/topics/what-is-blockchain

기말고사 과제

- Django를 이용하여 Web Server 구축
  - 본인의 홈페이지 또는 본인의 관심사 내용으로 웹페이지 작성
  - 본인이 작업한 내용을 github에 새로운 repository를 생성하여 관리
  - 무료 Cloud serve를 활용하거나 본인 PC에 서버를 구축하여 6월말까지 운영
  - 제출 : 번호_학번_이름_Django.ppt & github 주소 & 서버 IP
  - 기한 : 6월 21일까지

- Blockchin 이란?
  - 제출 : 번호_학번_이름_Blockchain.ppt
  - 기한 : 6월 21일까지