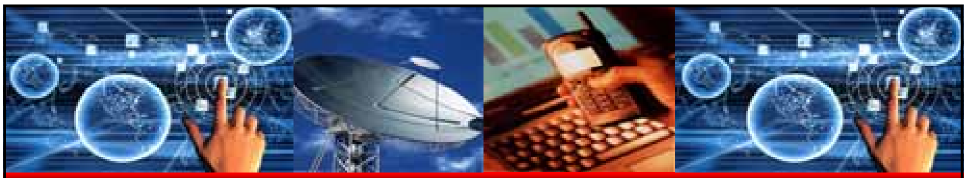


네트워크 보안
(Network Security)

2007. 9. 17

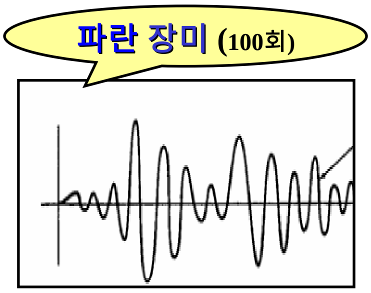
컴퓨터정보공학부
이 훈 재

발표 순서

- ✓암호 알고리즘
  - 암호의 역사
  - 암호 알고리즘(AES)
- ✓네트워크 보안
  - 방화벽(Firewall)
  - 전자우편 보안(PGP)
  - 웹보안(SSL/TLS/WTLS)
  - 네트워크 보안 프로젝트

선조들의 지혜 - 정보량 이론을 알고 있었다!

❖ **“百聞이 不如一見” ➔ 정보량(단위: 비트) 이론 해석**
“백번 듣는 것 보다 한번 보는 것이 낫다”



- 음성: 6.4Mbits
  (PCM 64kbps x 1sec x 100회)
- 영상: 56.6Mbits
  (1024 x 768 x 3RGB x 24 bit)

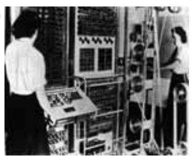
암호 알고리즘 - 암호의 역사

- **기원전 이집트 상형문자, <u>시저 암호</u>, Scytale**

- 1800. Vigenere cipher
- 1918. Vernam cipher = one-time pad
- 1917. Rotor Machine
- 1920. Enigma Machine, Hegelin Machine

- 1948. C.E.Shannon,“Secrecy System 이론” 정립
- 1970. Europe, “Stream Cipher” 설계/응용
- 1970. Fiestel, “LUCIFER”
- 1975. IBM, “**DES**”

- 1976. Diffie & Hellman, “Public-Key Cryptosystems”
- 1978. Rivest, Shamir & Adleman, “**RSA**”
- 1980-90 A5, RC4, skipjack, IDEA, **SEED**, ECC 등
- 2000- **AES**(Rijndael), Camelia, **ARIA** 등



Overview of Cryptography & Its Applications

- People wants and needs privacy and security while communicating
- In the past, cryptography is heavily used for military applications to keep sensitive information secret from enemies (adversaries). Julius Caesar used a simple shift cipher to communicate with his generals in the battlefield.
- Nowadays, with the technologic progress as our dependency on electronic systems has increased we need more sophisticated techniques.
- Cryptography provides most of the methods and techniques for a secure communication

0.1 Secure Communications

- Cryptography = "Secret Writing"
  암호 설계 (暗號 設計)
  - Designing of cryptosystems
- Cryptology = "Secret Learning"
  암호학 (暗號學)
  - Cryptography + Cryptanalysis
- Cryptanalysis = "Secret Analyzing"
  암호해독(暗號解讀) 또는 암호분석(暗號分析)
  - Breaking for cryptosystems

Terminology

Cryptology: All-inclusive term used for the study of secure communication over non-secure channels and related problems.

Cryptography: The process of designing systems to realize secure communications over non-secure channels.

Cryptanalysis: The discipline of breaking the cryptographic systems.

Coding Theory: Deals with representing the information using codes. It covers: compression, secrecy, and error-correction. Recently, it is predominantly associated with error-correcting codes which ensures the correct transmissions over noisy-channels.

The Aspects of Cryptography

• Modern cryptography heavily depends on mathematics and the usage of digital systems.

• It is a inter-disciplinary study of basically three fields:

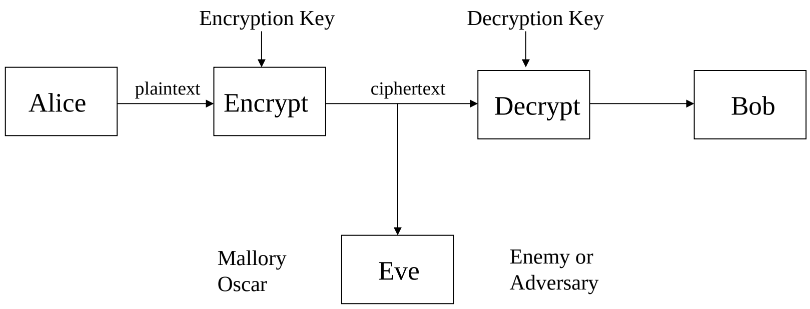
Mathematics
Computer Science
Electrical Engineering

• Without having a complete understanding of cryptoanalysis (or cryptoanalytic techniques) it is impossible to design *good* (secure, unbreakable) cryptographic systems.

• It makes use of other disciplines such as error-correcting codes compression.

Copyright © 2007 CNSLab.

Secure Communications



Basic Communication Scenario

Eve's Goals

Read the message

1. Figure out the key Alice is using and read all the messages encrypted with that key
2. Modify the content of the message in such a way that Bob will think Alice sent the altered message.
3. Impersonate Alice and communicate with Bob who thinks he is communicating with Alice.

Oscar is a passive observer who is trying to perform (1) and (2).

Mallory is more active and evil who is trying to perform (3) And (4).

Attack Methods

1. **Ciphertext only:** Alice has only a copy of ciphertext
2. **Known Plaintext:** Eve has a copy of ciphertext and the corresponding plaintext and tries the deduce the key.
3. **Chosen Plaintext:** Eve has a copy of ciphertext corresponding to a copy of plaintext selected by Alice who believes it is useful to deduce the key.
4. **Chosen Ciphertext:** Eve has a copy plaintext corresponding to a copy of ciphertext selected by Alice who believes it is useful to deduce the key.

Kerckhkoffs's Principle

While assessing the strength of a cryptosystem, one should always assume that **the enemy knows the cryptographic algorithm used**.

The security of the system, therefore, should be based on

* the quality (strength) of the algorithm but not its obscurity
  the key space (or key length)

Symmetric Key Algorithms

- Encryption and decryption keys are known to both communicating parties (Alice and Bob).
- They are usually related and it is easy to derive the decryption key once one knows the encryption key.
- In most cases, they are identical.
- All of the classical (pre-1970) cryptosystems are symmetric.
- Examples : DES and AES (Rijndael)

- A Secret should be shared (or agreed) btw the communicating parties.

Why public key cryptography ?

• Key Distribution and Management is difficult in Symmetric Cryptoystems (DES, 3DES, IDEA, AES(Rijndael) over large networks.

• No Electronic Signature with symmetric ciphers

• Public Key Cryptosystems provide functions for all four Security Services.

• Also makes it possible to implement Key Exchange, Secret Key Derivation, Secret Sharing functions.

Public Key Cryptosystems (PKC)

Each user has a pair of keys which are generated together under a scheme:

• Private Key - known only to the owner

• Public Key - known to anyone in the systems with assurance

Encryption with PKC:

Sender encrypts the message by the *Public Key* of the receiver

Only the receiver can decrypt the message by her/his *Private Key*

Non-mathematical PKC

Bob has a box and a padlock which only he can unlock once it is locked.

• Alice want to send a message to Bob.
• Bob sends its box and the padlock unlocked to Alice.
• Alice puts its message in the box and locks the box using Bob's padlock and sends the box to Bob thinking that the message is safe since it is Bob that can unlock the padlock and accesses the contents of the box.
• Bob receives the box, unlocks the padlock and read the message.

Attack:
However, Eve can replace Bob's padlock with hers when he is sending it to Alice.

Aspects of PKC

Powerful tools with their own intrinsic problems.

- Computationally intensive operations are involved.
- Resource intensive operations are involved.
- Implementation is always a challenge.
- Much slower than the symmetric key algorithms.
- PKC should not be used for encrypting large quantities of data.

Example PKCs

- RSA
- Discrete Logarithm based cryptosystems. (El-Gamal)
- Elliptic Curve Cryptosystems
- NTRU

Key Length in Cryptosystems

Following the Kerckhkoffs's Principle, the strength (security) of cryptosystems based on two important properties:

the quality of the algorithm

the key length.

- The security of cryptographic algorithms is hard to measure
- However, one thing is obvious: the key should be large enough to prevent the adversary to determine the key simply by trying all possible keys in the key space.
- This is called **brute force** or **exhaustive search attack.**

- For example, DES utilizes 56-bit key, therefore there are 2^{56} (or approx 7.2×10^{16}) possible keys in the key space.

Key Length in Cryptosystems

• Assume that there are 10^{30} possible key you need to try
• And you can only try 10^{9} key in a second.
• Since there are only around $3x10^{7}$ seconds in year brute force attack would take more than $3x10^{13}$ years to try out the keys. This time period is longer than the predicted life of the universe.

• For a cryptoanalyst, brute force should be the last resort.
• S/He needs to take advantage the weakness in the algorithm or in the implementation of it in order to reduce the possible keys to try out.

• Longer keys do not necessarily improve the security

Unbreakable Cryptosystems

• Almost all of the practical cryptosystems are theoretically breakable given the time and computational resources
• However, there is one system which is even theoretically unbreakable: **One-time-pad.**
• One-time pad requires exchanging key that is as long as the plaintext.
• However impractical, it is still being used in certain applications which necessitate very high-level security.
• Security of one-time pad systems relies on the condition that keys are generated using truly random sources.

Fundamental Cryptographic Applications

- **Confidentiality**

  Hiding the contents of the messages exchanged in a transaction

- **Authentication**

  Ensuring that the origin of a message is correctly identified

- **Integrity**

  Ensuring that only authorized parties are able to modify computer system assets and transmitted information

- **Non-repudiation**

  Requires that neither of the authorized parties deny the aspects of a valid transaction

Other Cryptographic Applications

- **Digital Signatures:** allows electronically sign (personalize) the electronic documents, messages and transactions
- **Identification:** is capable of replacing password-based identification methods with more powerful (secure) techniques.
- **Key Establishment:** To communicate a key to your correspondent (or perhaps actually mutually generate it with him) whom you have never physically met before.
- **Secret Sharing:** Distribute the parts of a secret to a group of people who can never exploit it individually.
- **E-commerce:** carry out the secure transaction over an insecure channel like Internet.
- **E-cash**
- **Games**

Copyright © 2007 CNSLab.

암호 알고리즘 - 개념

평문 → **암호알고리즘** → 암호문

비밀키 , 암호키, 키

키 정보를 알고 있는 사람만이 암호화와 복호화가 가능

관용키(Conventional)
비밀키(Secret-key)
대칭키(Symmetric-key)

암호화키 = 복호화키

DES , SKIPJACK , IDEA , AES, SEED, Camelia, ARIA

공개키(Public Key)
비대칭키(Asymmetric-key)

암호화키 ≠ 복호화키

RSA , ElGamal, ECC

암호 알고리즘 - 안전한 키 길이

❖ 암호 키 크기를 연도별 요약

[출처] A.K. Lenstra & E.R.Verheul, “Selecting Cryptographic Key Sizes” , PKC2000, Jan, 2000

연도	대칭키	RSA/DH	Subgroup	Elliptic Curve	MIPS Year	H/W cost
2000	70	952	125	132	7.13×10^{9}	1.39×10^{8}
2005	**74**	**1149**	**131**	**147**	**1.02×10^{11}**	**1.96×10^{8}**
2010	78	1369	138	160	1.45×10^{12}	2.77×10^{8}
2020	86	1881	151	188	2.94×10^{14}	5.55×10^{8}

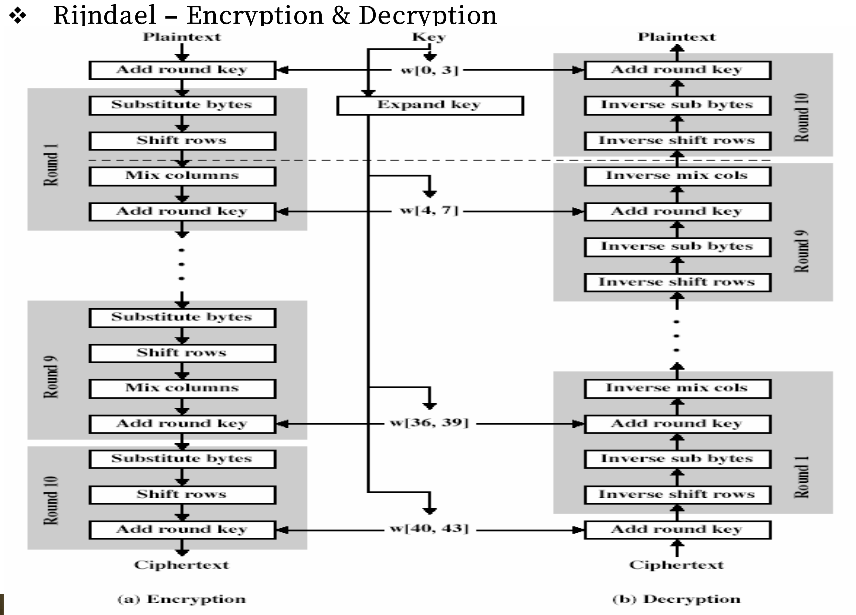
암호 알고리즘 - AES

- NIST FIPS-197, AES (Advanced Encryption Standard, 2001.11.26)
- 새로운 미국 암호 표준, DES 알고리즘(56-bit 키) 대체
- 설계자: Rijmen-Daemen (Belgium)
- 키크기: 128/192/256 bit keys
- 데이터 블록 크기:128 bit data
- 라운스 수: 10/12/14 rounds (iterations)
- 적합한 프로세서: 32-bit processor
- 수학이론배경: 확장 유한체 GF(2^8) with $p(x)=x^8+x^4+x^3+x+1$

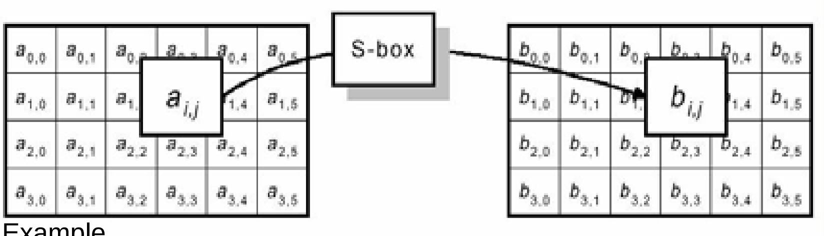
- 한국형 암호 표준화
  - ✓ SEED(1997, TTA 표준), ARIA(2004, 국가용 표준)
  - ✓ KC-DSA(1996, KSC 표준), HAS-160(1998, TTA 표준)
  - ✓ 차세대 암호 표준화 위원회 ➔ 개발 중 (블록, <u>스트림</u>, 공개키, 해쉬, 평가)

암호 알고리즘 - AES

- Rijndael – Encryption & Decryption



❖ Byte Substitution - Examples



– Example

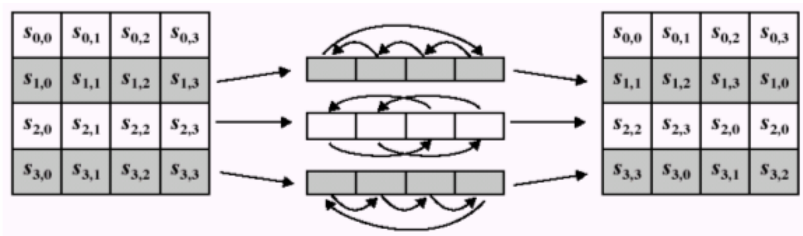
EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

암호 알고리즘 - AES

❖ Shift Rows



– Example

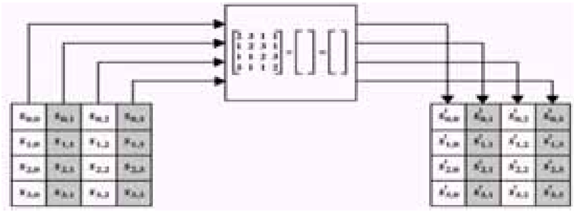
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Copyright © 2007 CNSLab.

❖ Mix Columns



– Example

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

❖ Add Round Key

– Example

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

⊕

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

네트워크 보안 – 보안 서비스

❖ Security Services:

- ✓ ***Confidentiality***: ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
- ✓ ***Authentication***: ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false
- ✓ ***Integrity***: ensures that only authorized parties are able to modify computer system assets and transmitted information
- ✓ ***Non-repudiation***: requires that neither the sender not the receiver of a message be able to deny the transmission
- ✓ ***Access control***: requires that access to information resources may be controlled by or for the target system
- ✓ ***Availability***: requires that computer system assets be available to authorized parties when needed

네트워크 보안 – 인터넷보안 종류

❖ 인터넷 보안 종류

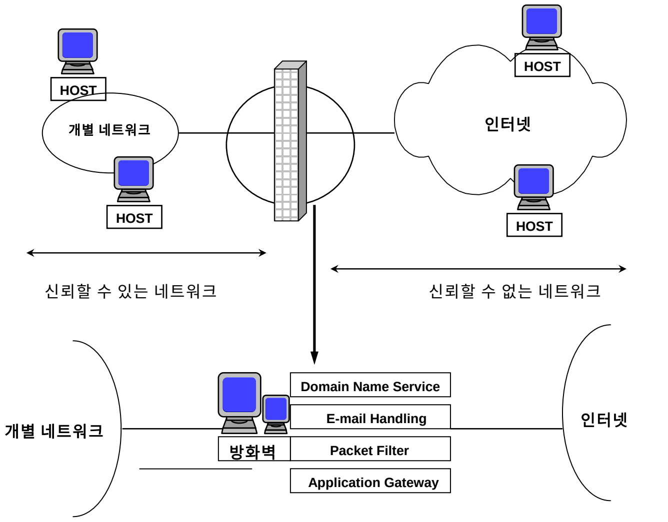
- ✓ Firewall(방화벽, 침입방어시스템)
  - – 패킷 필터링 방화벽
  - – 응용 게이트웨이 방화벽
- ✓ IDS (Intrusion Detection System, 침입탐지시스템)
- ✓ IPS (Intrusion Prevention System, 침입방지시스템)
- ✓ VPN(Virtual Private Network, 가상사설망)
- ✓ 전자메일보안(Secure E-mail)
  - – PEM
  - – PGP
- ✓ WWW 보안(Secure Web)
  - – S-HTTP (Secure HTTP)
  - – SSL (Secure Socket Layer)
  - – TLS (Transport Layer Security)
- ✓ 무선인터넷 보안 : WTLS (Wireless TLS)

Copyright © 2007 CNSLab.

네트워크 보안 – 방화벽

❖ **FireWall**

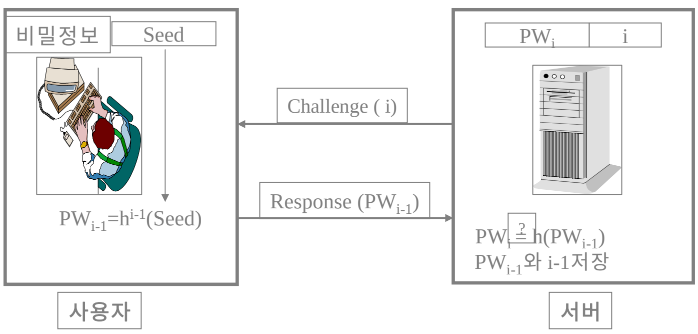
- ✓ 내부 네트워크에 대한 접속제어, 외부 네트워크로부터의 보호
- ✓ 라우터 또는 응용 게이트웨이에서 구현됨.
- ✓ 외부 네트워크와 내부 네트워크 사이에 허가된 트래픽 만 통과시킴



네트워크 보안 – 방화벽

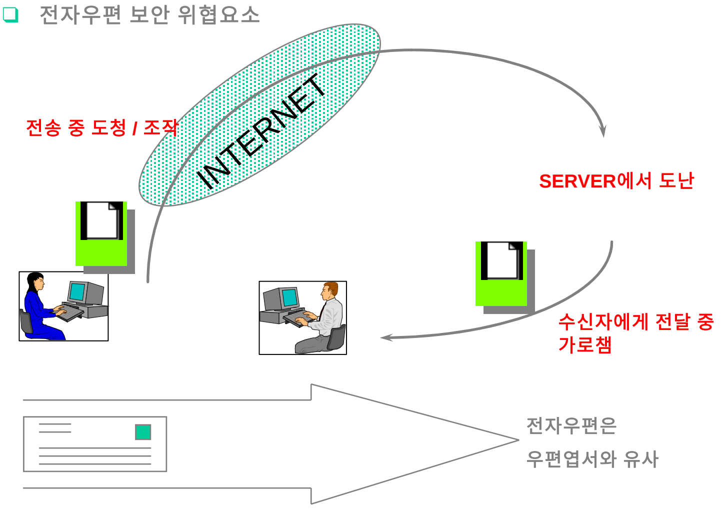
❖ 방화벽 인증기법

➢ **One-Time Password (S/KEY)**



네트워크 보안 – 전자우편 보안

- 전자우편 보안 위협요소



네트워크 보안 – 전자우편 보안

전자우편 보안 서비스

- 메시지 기밀성
- 송신자에 대한 실체인증
- 메시지 무결성
- 부인봉쇄

- **PEM** (Privacy Enhanced Mail)
- **PGP (Pretty Good Privacy)**
- **S/MIME(Secure/Multipurpose Internet Mail Extensions) , by RSA 사**
- **MOSS(MIME Object Security Service)**

❖ Pretty Good Privacy (PGP)

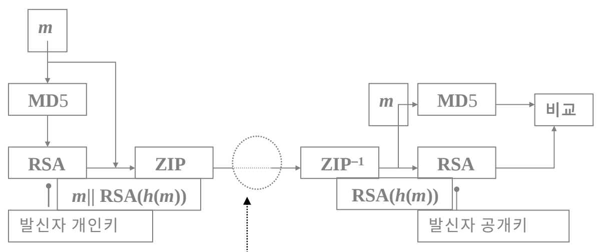
✓ PGP 기능과 알고리즘

기 능	사용된 알고리즘
기밀성	IDEA(메시지), RSA(세션키)
송신자 인증	RSA, MD5
압 축	ZIP

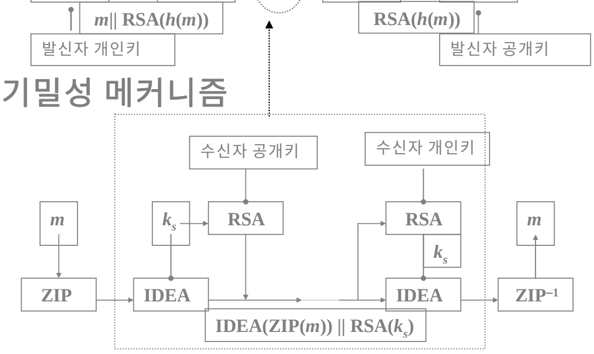
✓ 특징

- Phil R. Zimmerman이 개발
- 다양한 운영체제에서 사용
- 기밀성과 인증 기능을 가짐.

❑ PGP 디지털 서명 메커니즘

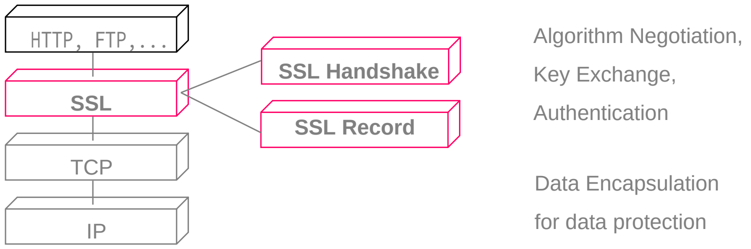


❑ PGP 기밀성 메커니즘



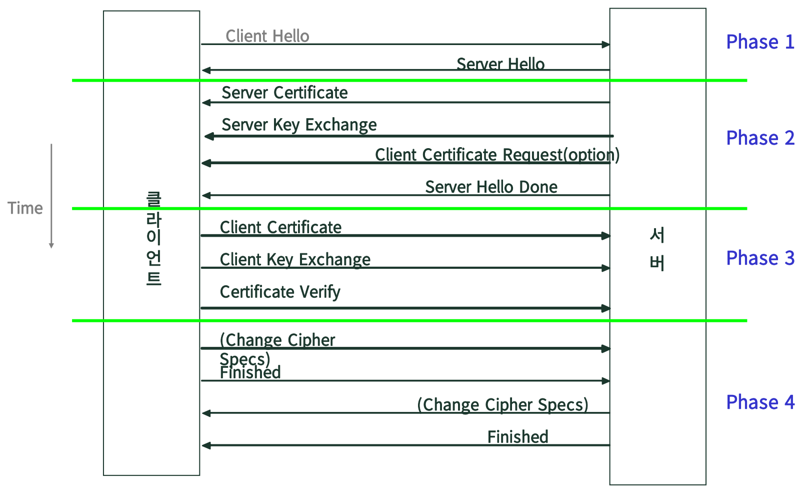
❑SSL (Secure Socket Layer) / TLS (Transport Layer Security)

- Netscape Communications
- Privacy, Data Integrity, Server [Client] Authentication,
- RSA, Diffie-Hellman, Fortezza for Key Exchange
- DES, 3DES, IDEA, RC2, RC4[stream cipher] for Data Encryption
- MD5, SHA for Hash Function (MAC)



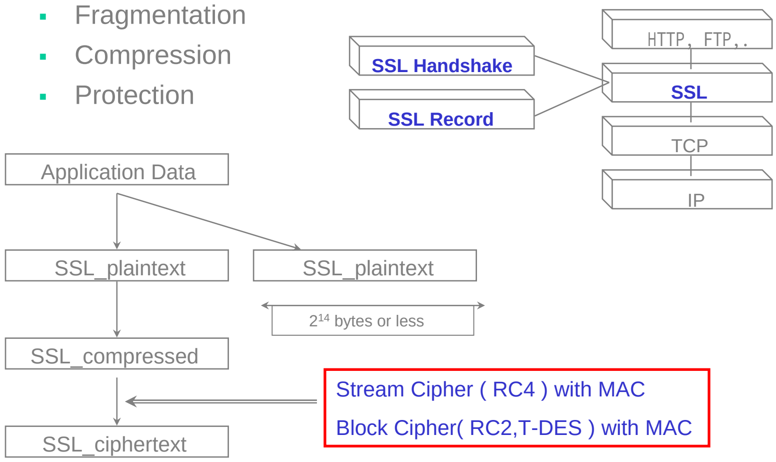
네트워크 보안 – 웹 보안

❑ (SSL/TLS) Handshake Protocol



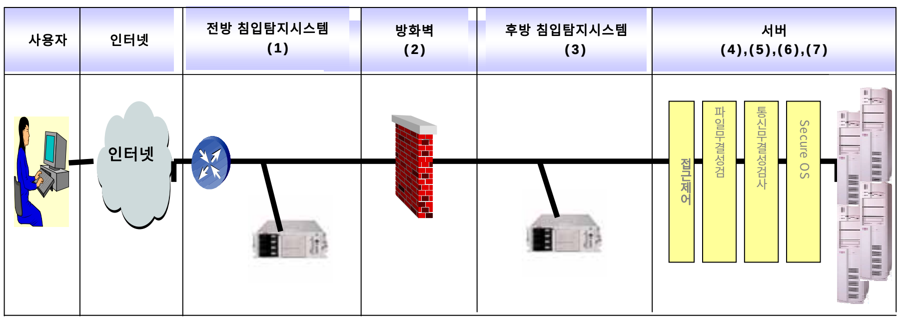
SSL/TLS Record Protocol

- Fragmentation
- Compression
- Protection



인터넷 해킹 및 보안

o 일반적인 7단계 인터넷 보안 구성의 예



□ 대학 보안네트워크 구성 예