Selected Topics

Dae Hyun Yum

Elliptic Curve Cryptography

타원곡선암호

Elliptic Curves

A Weierstrass equation defined over K K라는 수체계. GF(p^n)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

하지만 2와3은 아님 GF(p^n)에서 P는 2.3이아님

If the characteristic of K is not equal to 2 or 3, then the admissible change of variables

$$\begin{array}{cc} & x \qquad\qquad\qquad\qquad y \\ (x, y) \to & \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right) \\ \text{대입} & \end{array}$$

transforms E to the curve

정리하면 $$y^2 = x^3 + ax + b$$

where $a, b \in K$. The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$.

ㄴ판별식이라고 이해.

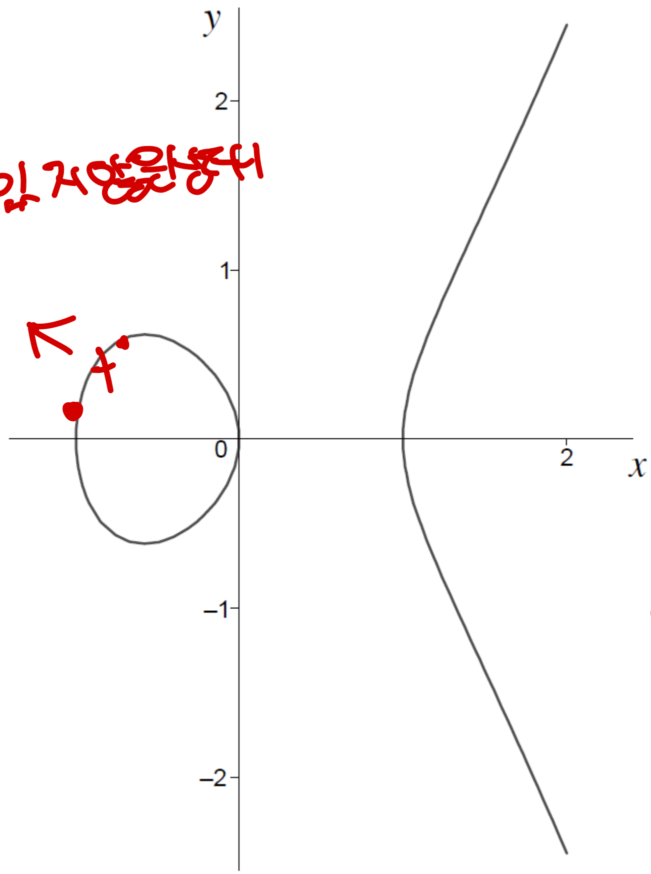
GF(p^n) a에 넣고 이해가능

discriminant가 0이 아닌 것을 원함

Elliptic Curves over R

닫혀있지 않은 형태

a



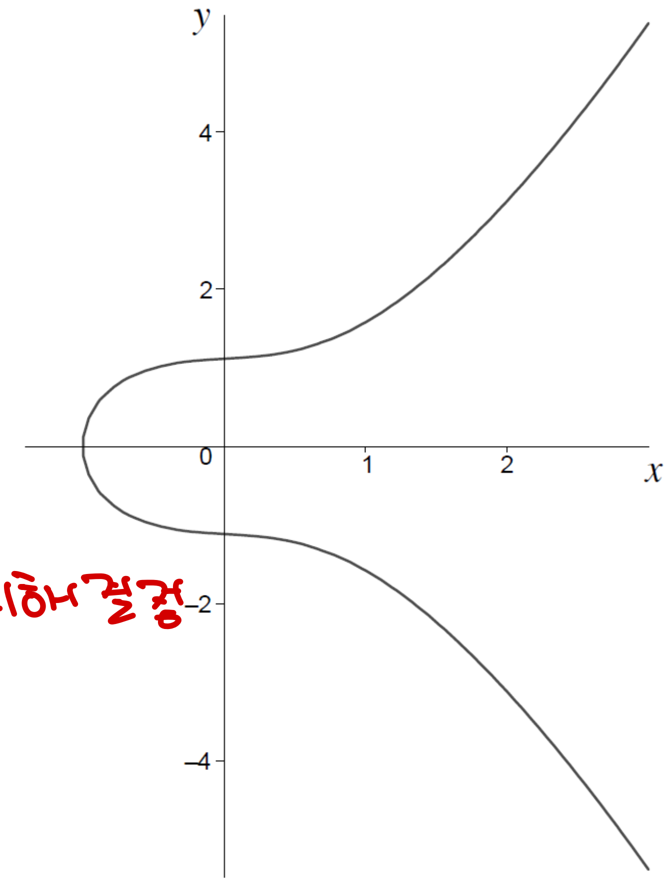
(a) $E_1 : y^2 = x^3 - x$

a
-1

3승이니까

dis는 양수

a b에 의해 결정

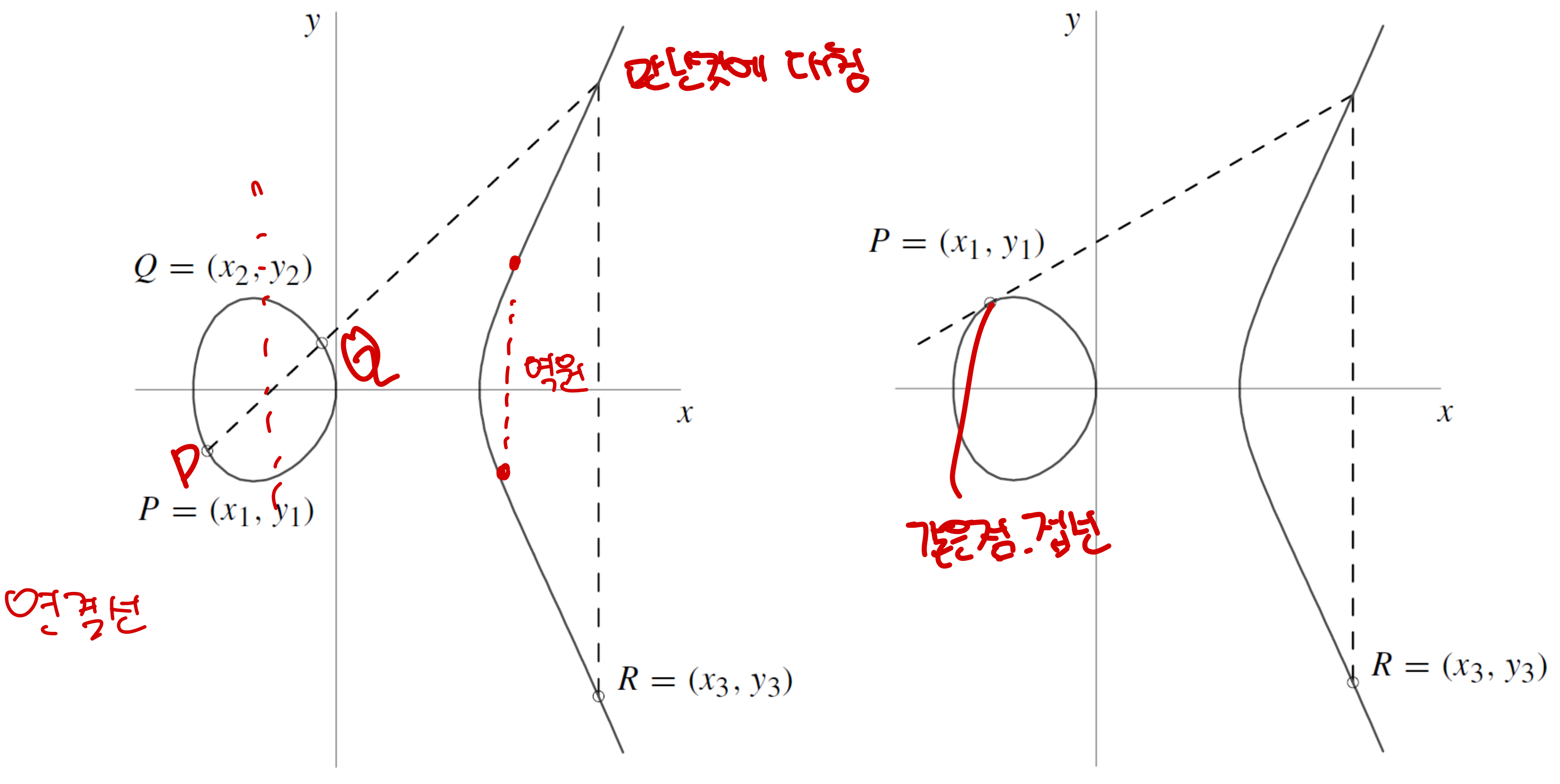


a
$\frac{1}{4}$

(b) $E_2 : y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$

dis는 음수

Group Law



(a) Addition: $P + Q = R$. (b) Doubling: $P + P = R$.

결합 교환 역원 항등원 모두성립. 수체계가 됨

Group Law

무한히 가면 만난다.

극한: ∞으로 두고 생각

Group law for $E/K: y^2 = x^3 + ax + b$, char$(K) \neq 2, 3$

새로운 점

항등원

1. *Identity*. $P + \infty = \infty + P = P$ for all $P \in E(K)$.

역원

2. *Negatives*. If $P = (x, y) \in E(K)$, then $(x, y) + (x, -y) = \infty$. The point $(x, -y)$ is denoted by $-P$ and is called the *negative* of P; note that $-P$ is indeed a point in $E(K)$. Also, $-\infty = \infty$.

더하기 ㄴ 성립

3. *Point addition*. Let $P = (x_1, y_1) \in E(K)$ and $Q = (x_2, y_2) \in E(K)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where 이 두 점을 더하려고 한다면

덧셈에 대한식

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

4. *Point doubling*. Let $P = (x_1, y_1) \in E(K)$, where $P \neq -P$. Then $2P = (x_3, y_3)$, where

덧셈 좌표

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad \text{and} \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

GROUP이 됨

Elliptic Curves over Finite Fields

$$E : y^2 = x^3 + 4x + 20$$

29로 나눈 나머지 집합

defined over $\mathbb{F}_{29}$. Note that $\Delta = -16(4a^3 + 27b^2) = -176896 \not\equiv 0 \pmod{29}$, so E is indeed an elliptic curve. The points in $E(\mathbb{F}_{29})$ are the following:

타원곡선

∞	$(2,6)$	$(4,19)$	$(8,10)$	$(13,23)$	$(16,2)$	$(19,16)$	$(27,2)$
$(0,7)$	$(2,23)$	$(5,7)$	$(8,19)$	$(14,6)$	$(16,27)$	$(20,3)$	$(27,27)$
$(0,22)$	$(3,1)$	$(5,22)$	$(10,4)$	$(14,23)$	$(17,10)$	$(20,26)$	
$(1,5)$	$(3,28)$	$(6,12)$	$(10,25)$	$(15,2)$	$(17,19)$	$(24,7)$	
$(1,24)$	$(4,10)$	$(6,17)$	$(13,6)$	$(15,27)$	$(19,13)$	$(24,22)$	

Examples of elliptic curve addition are $(5,22) + (16,27) = (13,6)$, and $2(5,22) = (14,6)$.

좌표끼리 더하라고 하면 4번식에 넣어서 계산

연산자가 하나는 GROUP. 결합. 역원. 항등원 존재

$x^3+ax+b.$ $x=0\sim22$

$E_{23}(1, 1)$: $y^2 = x^3 + x + 1$ over F_{23}

$x=1,\ y=7$

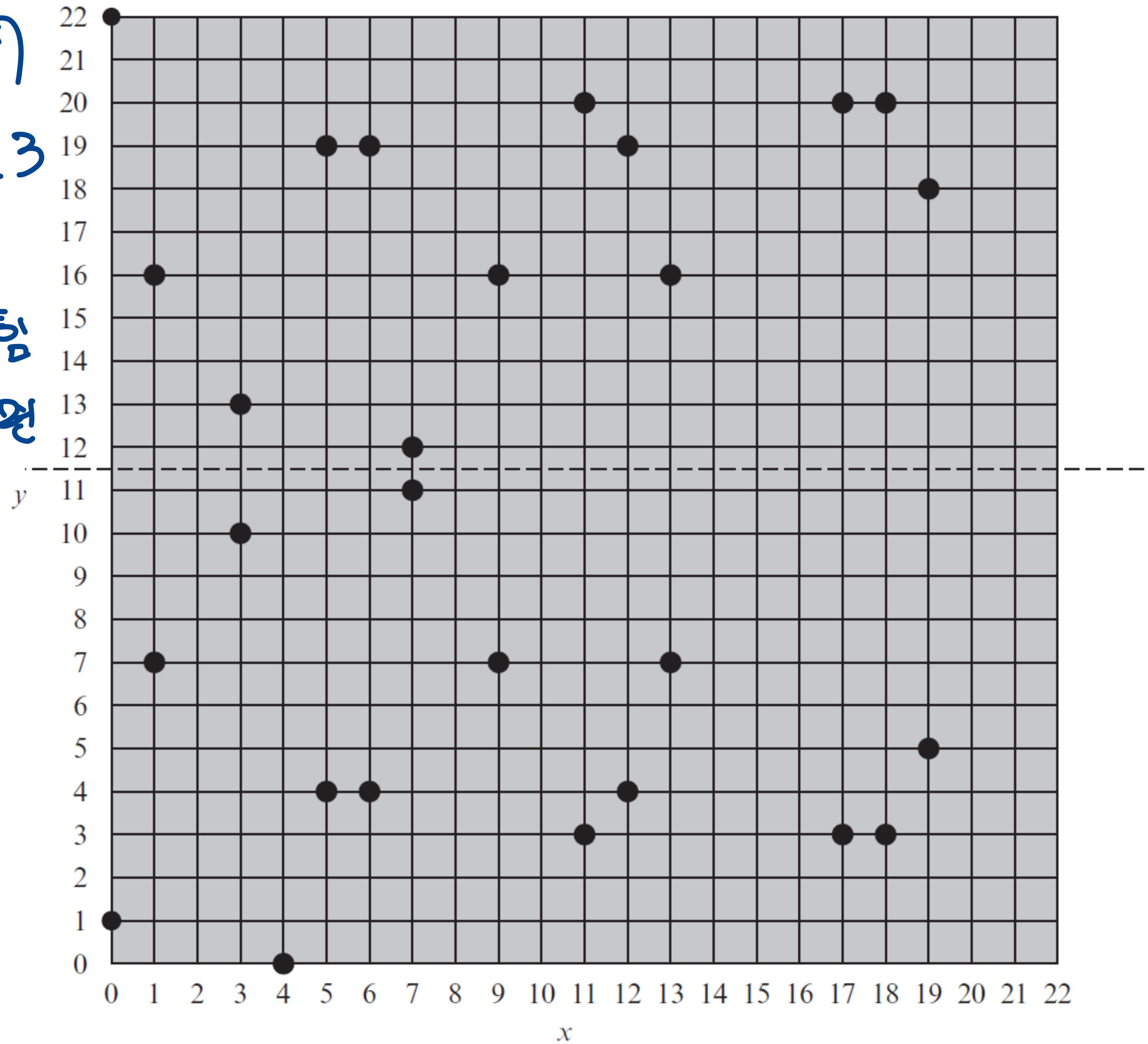
$49\div23=2\dots3$

식 성립

점이 2개씩 짝임

그 2개를 더하면

23이된다.



$E_{23}(1, 1)$: $y^2 = x^3 + x + 1$ over F_{23}

Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.

For example, let $P = (3, 10)$ and $Q = (9, 7)$ in $E_{23}(1, 1)$. Then

$$\lambda = \left(\frac{7 - 10}{9 - 3}\right) \bmod 23 = \left(\frac{-3}{6}\right) \bmod 23 = \left(\frac{-1}{2}\right) \bmod 23 = 11$$

$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$

$$y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$$

So $P + Q = (17, 20)$. To find $2P$,

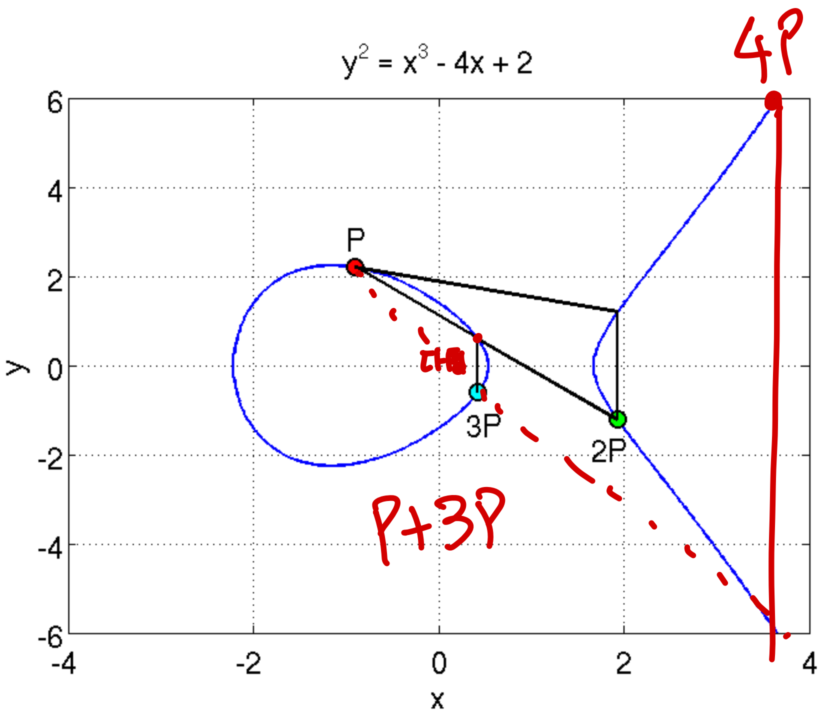
$$\lambda = \left(\frac{3(3^2) + 1}{2 \times 10}\right) \bmod 23 = \left(\frac{5}{20}\right) \bmod 23 = \left(\frac{1}{4}\right) \bmod 23 = 6$$

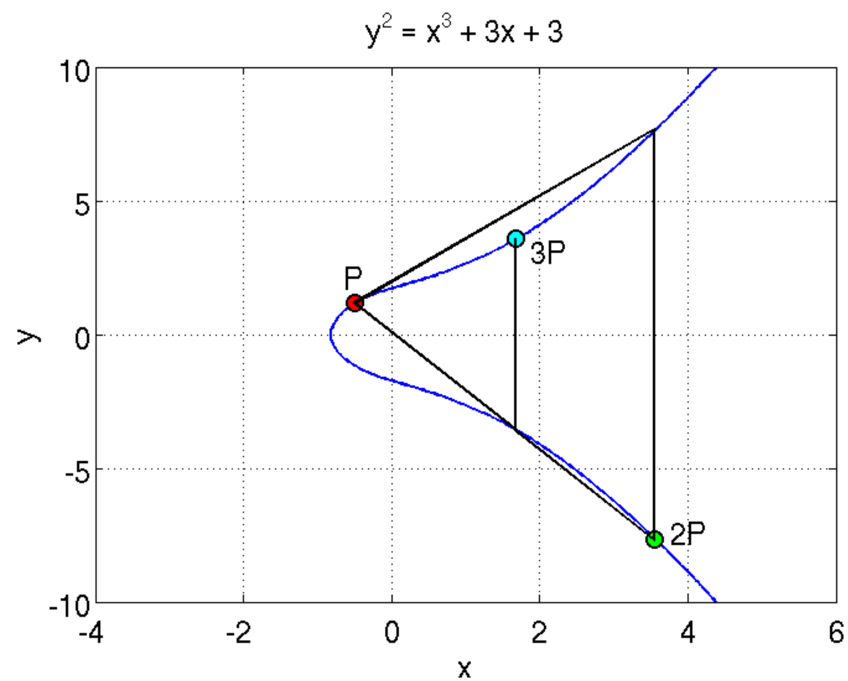
$$x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$$

$$y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$$

$$2P = (7, 12).$$

Elliptic Curve Point Addition/Doubling



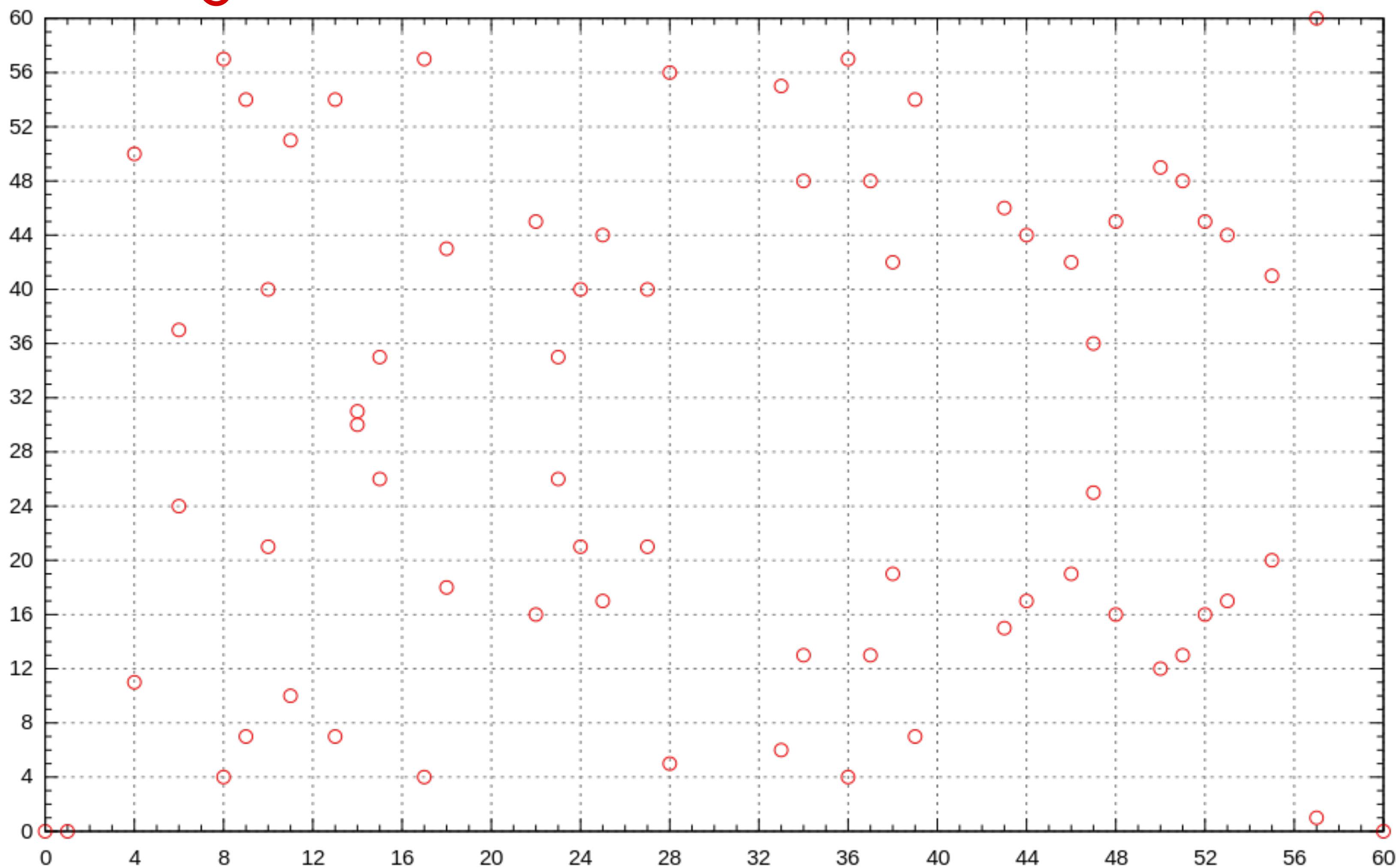


$Y = xG$ G를 x번 더하기. 점들간의 이산대수문제

$y = g^x \bmod p$

$E_{61}(-1, \cancel{-1})$: $y^2 = x^3 - x$ over F_{61} $x = 0 \sim 60$

0



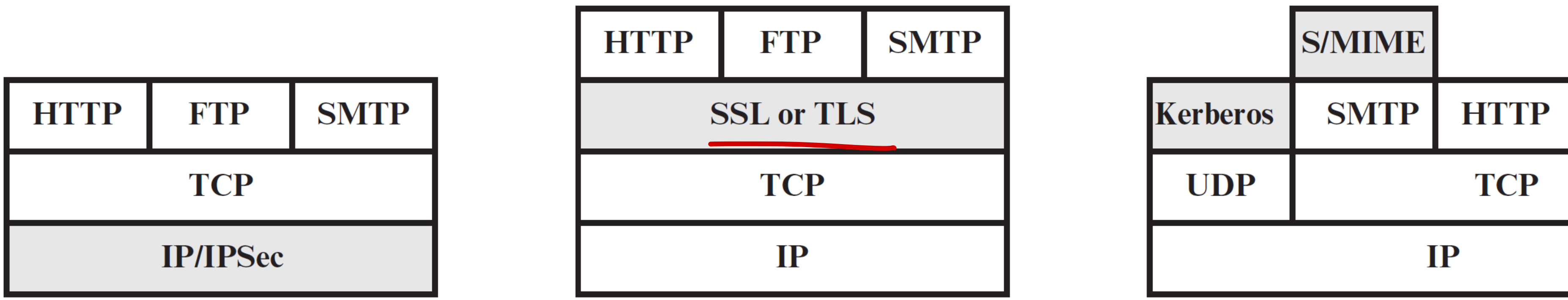
ECDH (Elliptic-Curve Diffie-Hellman)

- Scheme

1. Alice and Bob agree on an elliptic curve E over a large finite field F and a point P on E.
2. Alice chooses a random integer a and sends $pk_A = aP$ to Bob.
3. Bob chooses a random integer b and sends $pk_B = bP$ to Alice.
4. Alice computes $a(pk_B) = a(bP) = abP$.
5. Bob computes $b(pk_A) = b(aP) = abP$.

Network Security: SSL/TLS

Relative Location of Security Facilities in the TCP/IP Protocol Stack



(a) Network level (b) Transport level (c) Application level

HTTPS

SSL를 사용함

SSL/TLS

- SSL/TLS   SSL을 거쳐서 와야함
  - Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.
  - Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP).
  - Websites can use TLS to secure all communications between their servers and web browsers.
  - The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.

SSL

예전 인터넷 툴

- Secure Sockets Layer (SSL)
  - Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the "father of SSL."

    헬먼제자
  - SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws.
  - Released in 1996, SSL version 3.0 represented a complete redesign of the protocol.

    충분히 안전

1.0-1.1은 지금볼때 안전하지 않음

TLS

SSL이 이름바꿈 SSL3.0

- Transport Layer Security (TLS)
  - TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0".
  - TLS 1.1 was defined in RFC 4346 in April 2006.
  - TLS 1.2 was defined in RFC 5246 in August 2008. - 현업에서 가장많이 호환
  - TLS 1.3 was defined in RFC 8446 in August 2018.
  - The PCI Council suggested that organizations migrate from TLS 1.0 to TLS 1.1 or higher before June 30, 2018.
  - In October 2018, Apple, Google, Microsoft, and Mozilla jointly announced they would deprecate TLS 1.0 and 1.1 in March 2020.

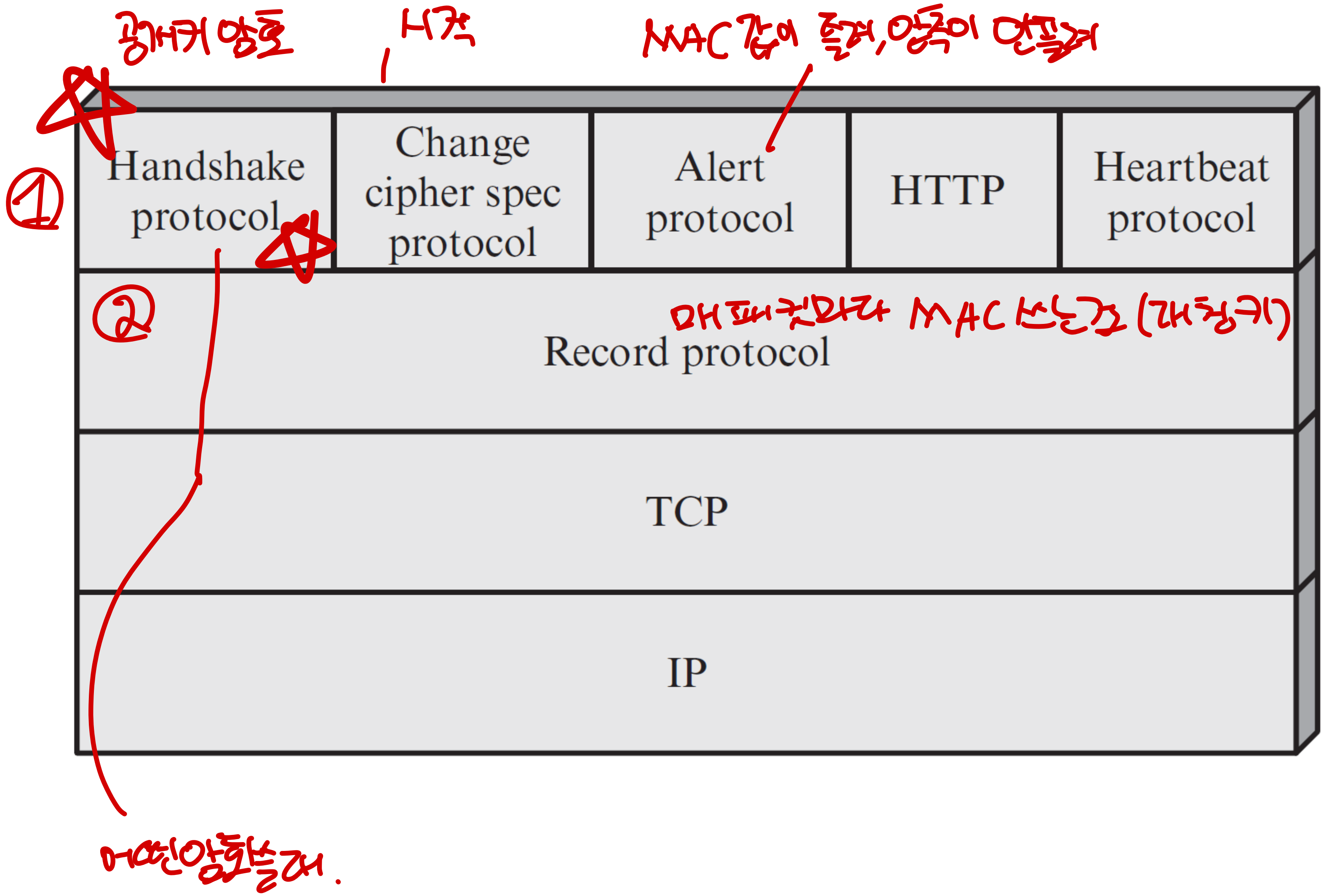
SSL and TLS Protocols

Protocol	Published	Status
SSL 1.0 표준된적없음	-	-
SSL 2.0	1995	Deprecated in 2011
SSL 3.0 퇴사	1996	Deprecated in 2015
TLS 1.0	1999	Deprecated in 2021
TLS 1.1	2006	Deprecated in 2021
TLS 1.2	2008	가장많이 지원
TLS 1.3	2018	

Protocol Overview

- The TLS protocol exchanges records, which encapsulate the data to be exchanged in a specific format.
- Each record can be compressed, padded, appended with a message authentication code (MAC), or encrypted, all depending on the state of the connection. 하이브리드 AES 키변교대칭이용 AES.MAC 7 대칭 최소
- Each record has a content type field that designates the type of data encapsulated, a length field and a TLS version field.
- The specifications (cipher suite, keys etc.) required to exchange application data by TLS, are agreed upon in the "TLS handshake" between the client requesting the data and the server responding to requests.

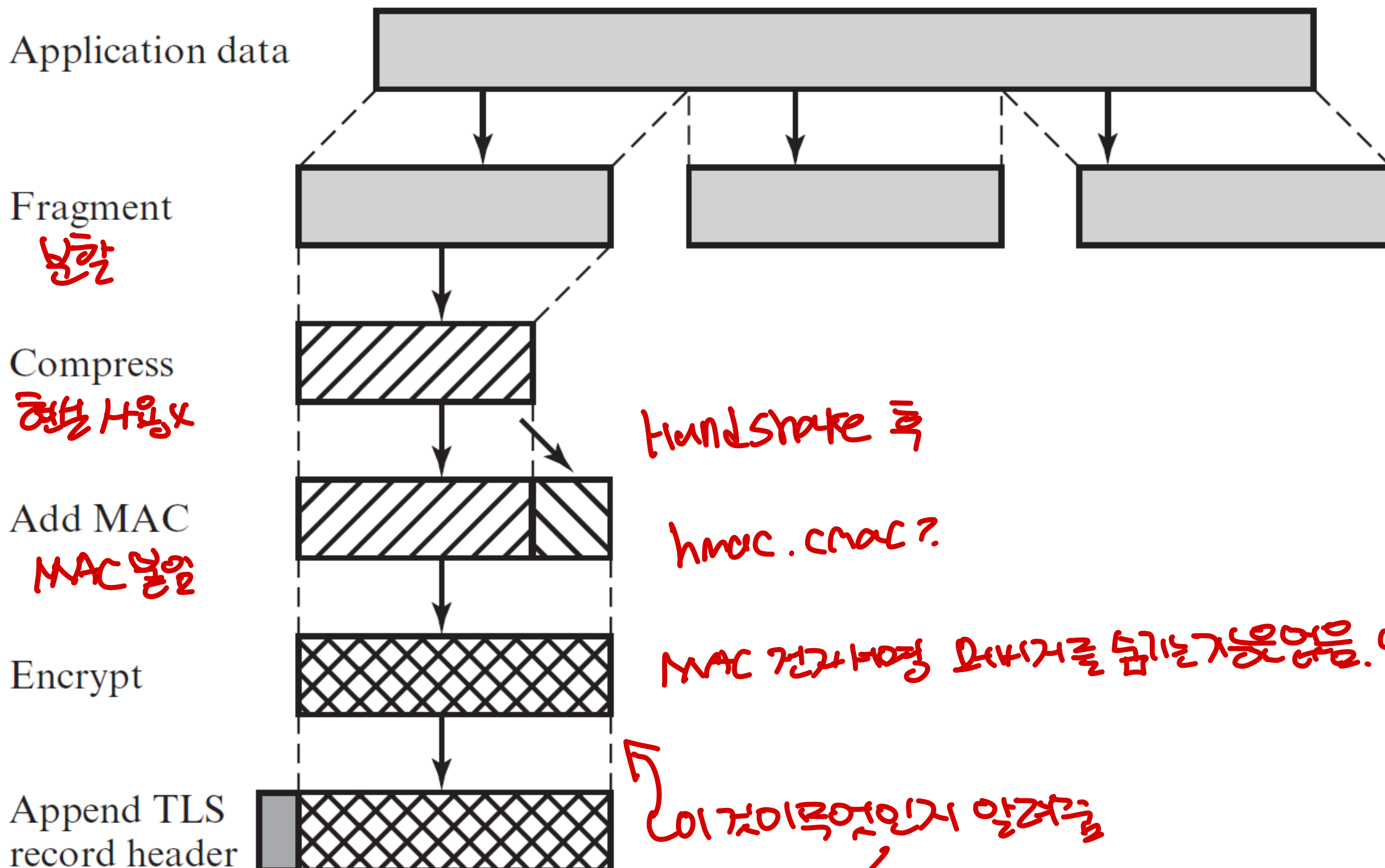
TLS Protocol Stack



TLS Record Protocol

- The TLS Record Protocol provides two services for TLS connections:
  - Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of TLS payloads.
  - Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC). 대칭형
- Overall operation
  - The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.

TLS Record Protocol Operation



분할

현재 사용x

MAC 붙임

Handshake 후

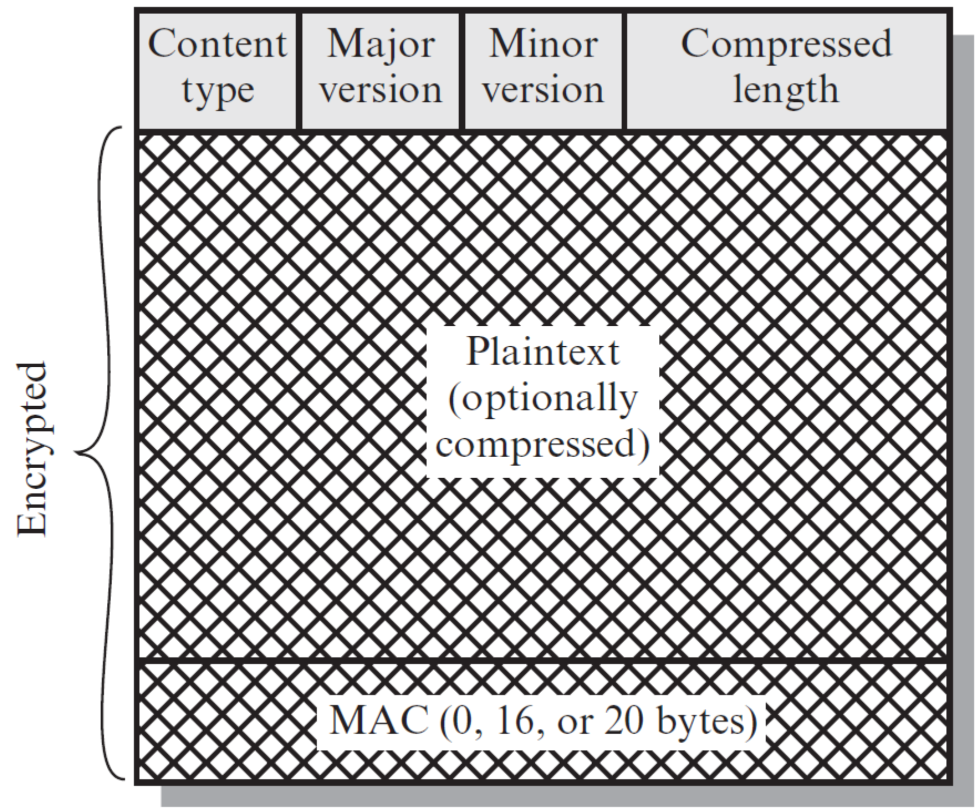
hmac, cmac?

MAC 결과 내용 오비기를 숨기는 기능은 없음. 암호화

이것이 무엇인지 알려줌

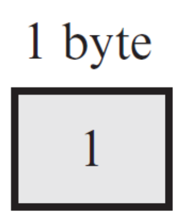
TLS Record Format

- Header
  - Content type (8 bits)
  - Major version (8 bits)
  - Minor version (8 bits)
  - Compressed length (16 bits)



Change Cipher Spec Protocol

- Change Cipher Spec Protocol
  - The Change Cipher Spec Protocol is one of the four TLS-specific protocols that use the TLS Record Protocol, and it is the simplest. This protocol consists of a single message, which consists of a single byte with the value 1. The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.



Change Cipher Spec Protocol

Alert Protocol

- Format
  - Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
  - If the level is fatal, TLS immediately terminates the connection.

이런일이 일어나면 session 끊어버림

    - unexpected_message
    - bad_record_mac 위변조
    - decompression_failure 압축이 안풀림
    - handshake_failure
    - illegal_parameter
    - decryption_failed
    - …

1 byte	1 byte
Level	Alert

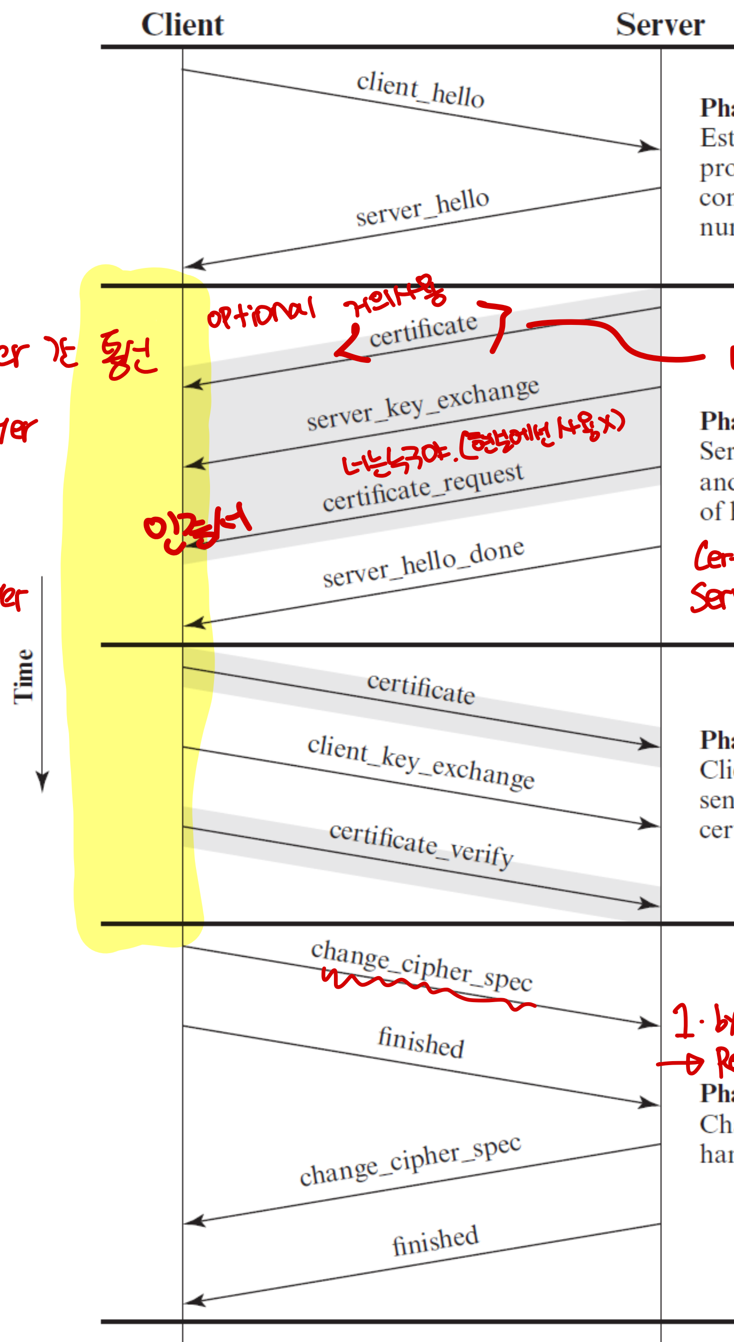
Handshake Protocol

- Overview
  - This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in a TLS record.
  - Each message has three fields:
    - Type (1 byte): Indicates one of 10 message types.
    - Length (3 bytes): The length of the message in bytes.
    - Content (≥ 0 bytes)

1 byte	3 bytes	≥ 0 bytes
Type	Length	Content

TLS Handshake Protocol Message Types

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

브라우저 — server 간 통신
└ Transport Layer
홈페이지 로그인
└ Application Layer

optional 거의사용
인증서
너는누구야. (현실에선 사용X)

서로 자신의 버전 등 완료
나는 누구야. 증명 TLS를 사용하려면 돈을 줘야함
Certificate를 안쓰면 Server가 내가 누군지 확인 안함.

서로 비밀키가 생성됨.
1 byte 시작한다는 것
→ Record protocol 시작!

Hello Messages

- client_hello or server_hello message has the following parameters:
  - Version: The highest TLS version understood by the client. 사용할 수 있는 TLS의 가장 높은 버전
  - Random: A client-generated random structure consisting of a 32-bit timestamp and 28 bytes generated by a secure random number generator. 32- 현재시간 나중에 다시 못쓰게 ran-28-byte
  - Session ID: A variable-length session identifier. 키 재생성X 처음엔 줄거고
  - CipherSuite: This is a list that contains the combinations of cryptographic algorithms supported by the client, in decreasing order of preference. ~버전 지원
  - Compression Method: This is a list of the compression methods the client supports.

CipherSuiteKey: Exchange Method Algorithms

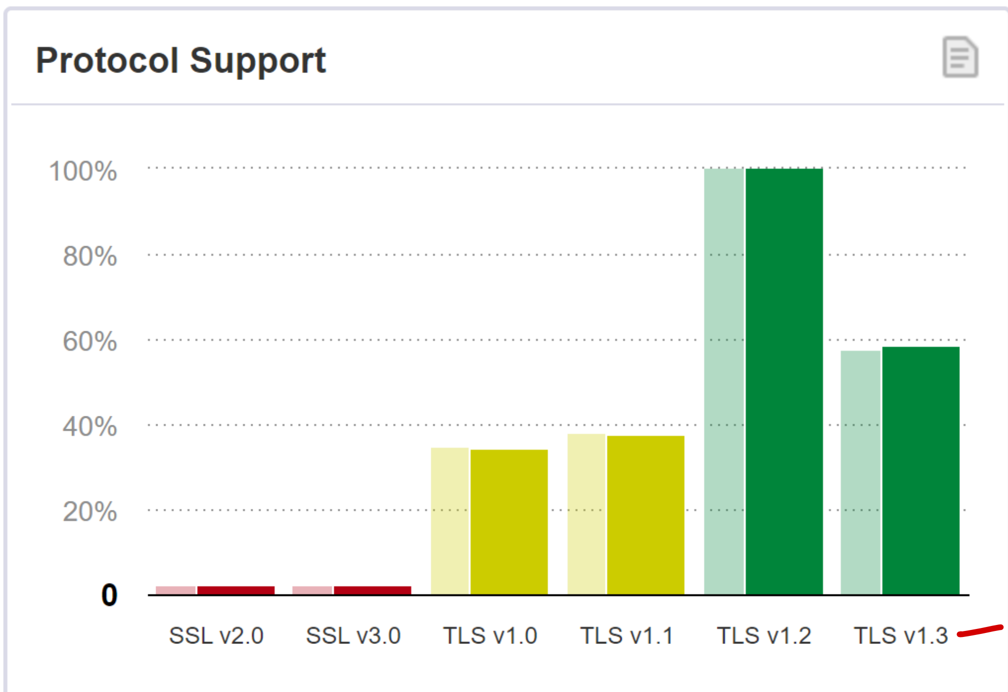
Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
DH-DSS	No	Yes	Yes	Yes	Yes	No
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No[58]
ECDH-ECDSA	No	No	Yes	Yes	Yes	No
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes
ECDH-EdDSA	No	No	Yes	Yes	Yes	No
ECDHE-EdDSA (forward secrecy)[59]	No	No	Yes	Yes	Yes	Yes
PSK	No	No	Yes	Yes	Yes	?
PSK-RSA	No	No	Yes	Yes	Yes	?
DHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes
ECDHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes
SRP	No	No	Yes	Yes	Yes	?
SRP-DSS	No	No	Yes	Yes	Yes	?
SRP-RSA	No	No	Yes	Yes	Yes	?
Kerberos	No	No	Yes	Yes	Yes	?
DH-ANON (insecure)	No	Yes	Yes	Yes	Yes	?
ECDH-ANON (insecure)	No	No	Yes	Yes	Yes	?
GOST R 34.10-94/34.10-2001[60]	No	No	Yes	Yes	Yes	?

매번 값이 바뀜

고정된 값 쓰지 마셈

SSL Pulse (https://www.ssllabs.com/ssl-pulse/)

- Websites
  - A primary use of TLS is to secure World Wide Web traffic between a website and a web browser encoded with the HTTP protocol. This use of TLS to secure HTTP traffic constitutes the HTTPS protocol.

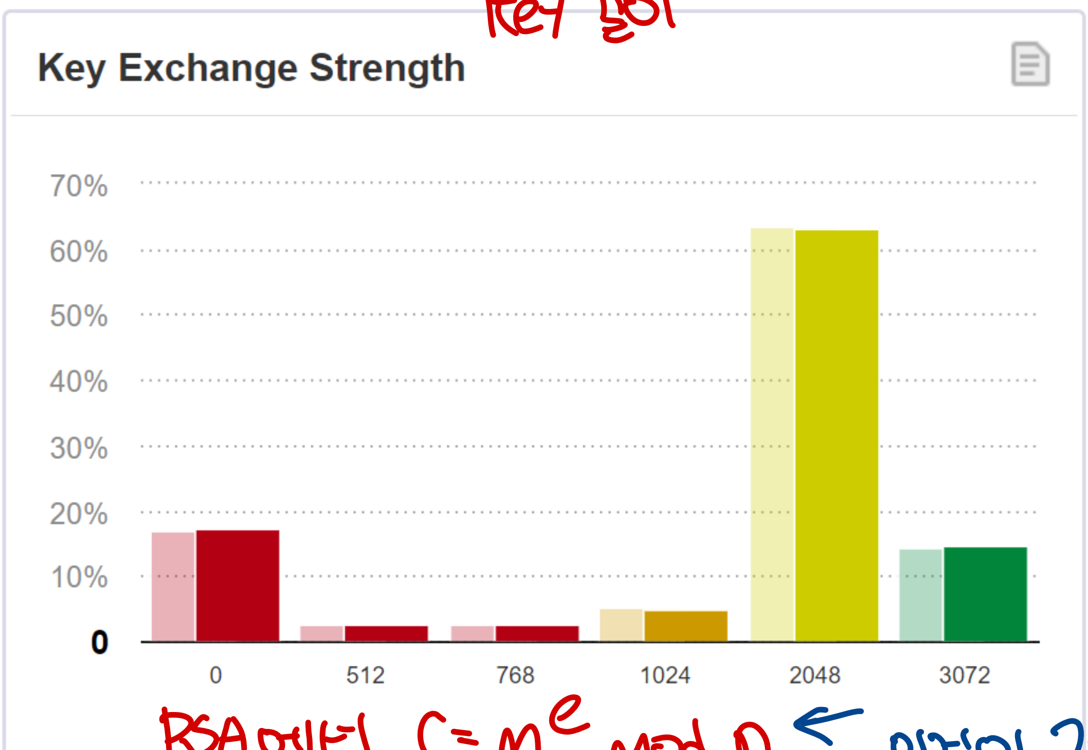


지원 60%

October & November (2022)

- The weakest key exchange supported by the servers SSL Pulse monitors.
- Currently, 2048 bits is the minimum expected strength.

key 길이



RSA에서 $C = m^e \bmod n$

$y = g^x \bmod p$

이것이 2048