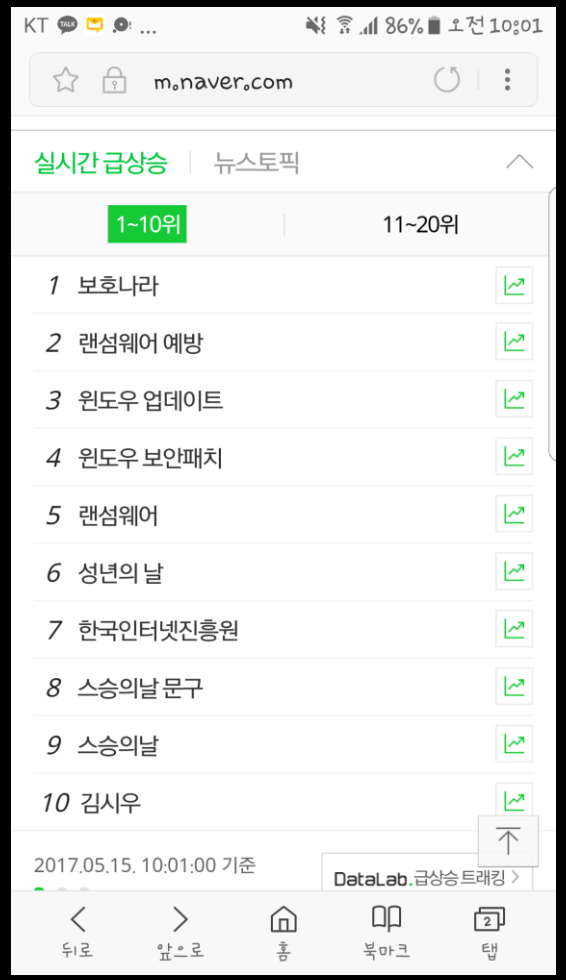
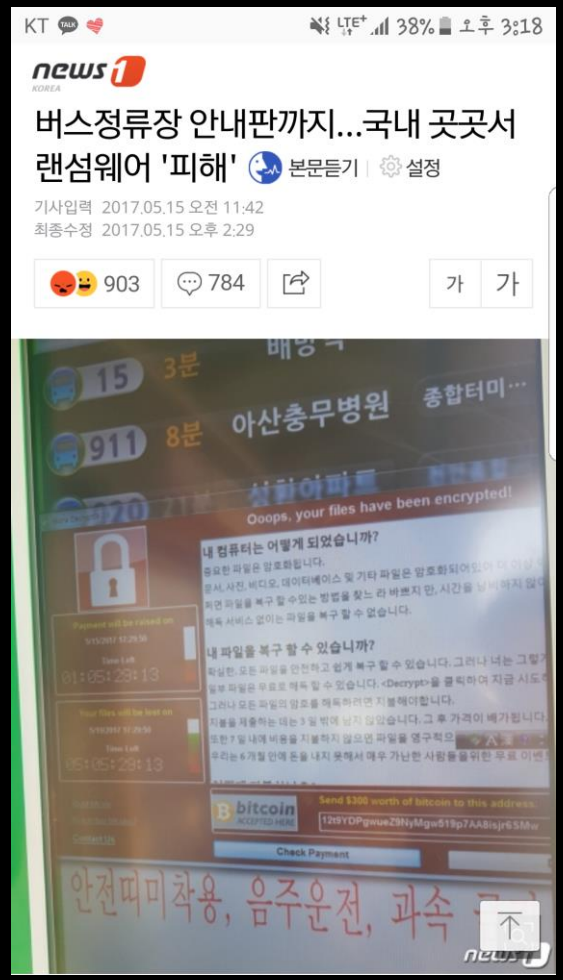
- 아월 말단 정지훈

암호학 알고리즘

발표자 소개

- 16년 아이스월 새터 조
- 16년 2학기 아이스월 가입
- 끝! -.- ㅎㅎ


KT ... 86% 오전 10:01
m.naver.com
실시간 급상승 | 뉴스토픽
1~10위 | 11~20위
1 보호나라
2 랜섬웨어 예방
3 윈도우 업데이트
4 윈도우 보안패치
5 랜섬웨어
6 성년의 날
7 한국인터넷진흥원
8 스승의날 문구
9 스승의날
10 김시우
2017.05.15. 10:01:00 기준
DataLab.급상승 트래킹
뒤로
앞으로
홈
북마크
탭


KT 38% 오후 3:18
news1
KOREA
버스정류장 안내판까지...국내 곳곳서 랜섬웨어 '피해'
본문듣기 | 설정
기사입력 2017.05.15 오전 11:42
최종수정 2017.05.15 오후 2:29
903
784
가 가
15 3분
911 8분
아산충무병원
종합터미...
Ooops, your files have been encrypted!
내 컴퓨터는 어떻게 되었습니까?
내 파일을 복구 할 수 있습니까?
bitcoin
Check Payment
안전띠미착용, 음주운전, 과속


KT ... 86% 오전 10:01
NAVER
세계 각국 '랜섬웨어' 피해 확산
SBS
[박진호의시사전망대] "가정도 병원도, 윈도우 쓰는 곳은 모두 조심해야"
본문듣기 | 설정
기사입력 2017.05.15 오전 9:16
최종수정 2017.05.15 오전 9:24
32
119
가 가
박진호의
시사 전망대
인터뷰 자료의 저작권은 SBS라디오에 있습니다. 전문 게재나 인터뷰 인용 보도 시, 아래와 같이 채널명과 정확한 프로그램명을 밝혀주시기 바랍니다.

대칭 KEY 암호

- 암호화와 복호화에 같은 암호 키
- 암호화 하는 측과 복호화 하는 측이 같은 암호 키 공유

송신자

대칭키
알고리즘

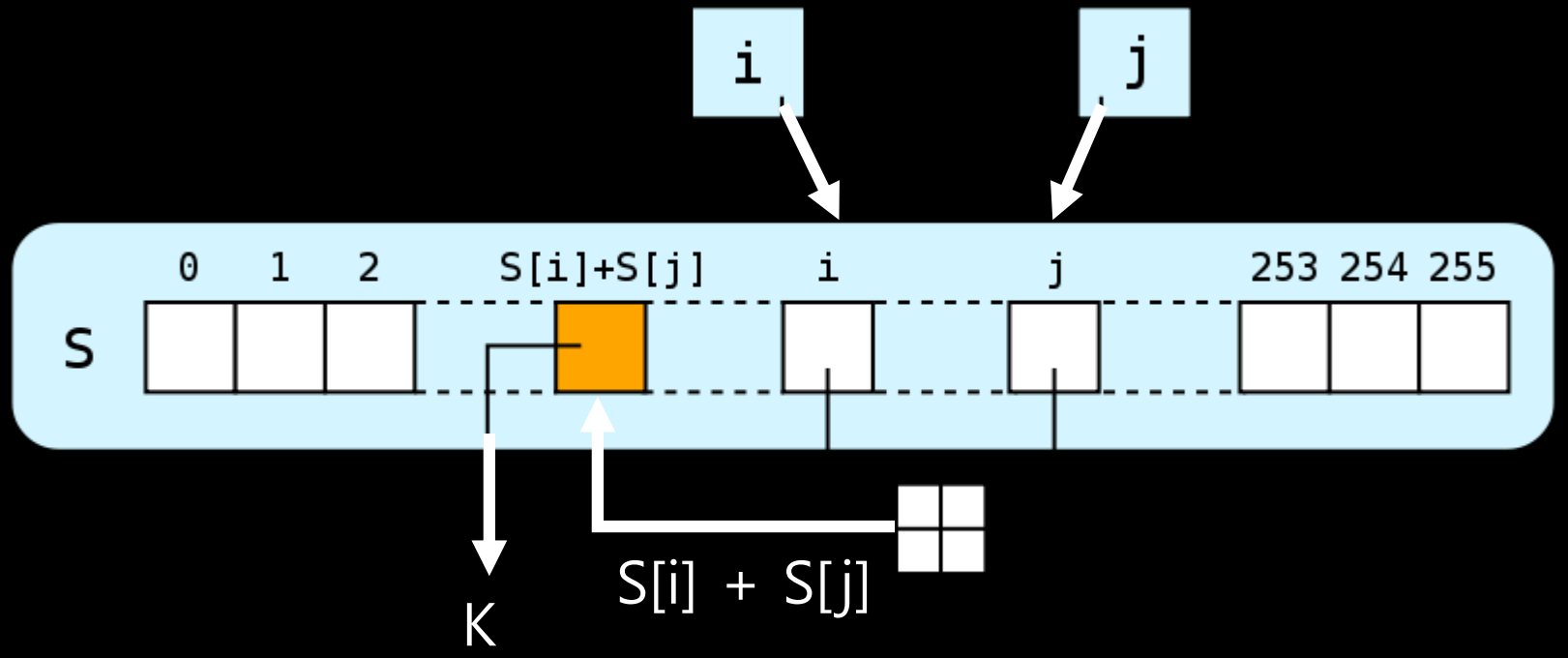
대칭키
알고리즘

수신자

암호문

암호문

스트림 암호



문제점

- 키 교환으로 문제 생김

송신자

수신자

대칭 KEY 종류

- DES
- AES
- ARIA
- SEED
- 등등

AES (고급 암호화 표준)


PROSOFT :: 암호화 알고
카피캣의 쉬운 암호학 ::
TLS - 나무위키
Advanced Encryption St
안전함 | https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
앱 새 탭 slader 객지 홈페이지 Google 설문지 slackbot | ICE 보고서 제출 Java Reffrence PROSOFT :: 암호화 암호화 -
3. AddRoundKey.
The SubBytes step [edit]
In the SubBytes step, each byte with a SubByte $S(a_{i,j})$ using an 8-bit sub ox. This operation provides the non-li erived from the multiplicative inve ve good non-linearity properties. To avoi rties, the S-box is construc unction with an invertible affine transformation. The oints (and so is a de i,j, and also any opposite fixed points, i.e., $S(a_{i,j}) \oplus a_{i,j}$ n, the InvSu Bytes) is used, which requires first taking the inverse of the affin ltiplic
The ShiftRows step [edit]
The ShiftRows step operates on the rows of the state; set. For AES, the first row is left unchanged. Each byte of the second row is shifted one to shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shi left circular by $n-1$ bytes. In this way, each column of the output state of the ShiftRows step is compos t state. (Rijndael variants with a larger block size have slightly different offsets). For a 256-bit block, the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only appl block, as AES does not use 256-bit blocks. The importance of this step is to avoid the col rates into four independent block ciphers.
The MixColumns step [edit]
Main article: Rijndael mix columns
In the MixColumns step, the four bytes o combined using an inve s function takes four bytes as input and output byte affects all four output by provides diffusion in the cipher.
During this operation, each co fixed matrix (matrix left-multiplied by column g the state):
$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$
Matrix multiplication is composed of multiplication and addition of the entries. Entries are 8 bit bytes treated as coefficients of polynomial of order
SubBytes
S
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.
No change
Shift 1
Shift 2
Shift 3
ShiftRows
In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.
MixColumns
⊗c(x)
In the MixColumns step, each column of the state is
오후 10:07
2017-05-15

공개 KEY 암호

- 사전에 비밀 키를 나눠 가지지 않은 유저가 안전하게 통신
- 공개 키는 누구나 but 비밀 키는 소유자만 그 둘은 달라야함
- B가 A의 공개키를 가지고 암호화하면 A는 그 문서를 자신만의 비밀 키를 가지고 복호화 한다.

송신자

공개 키
알고리즘

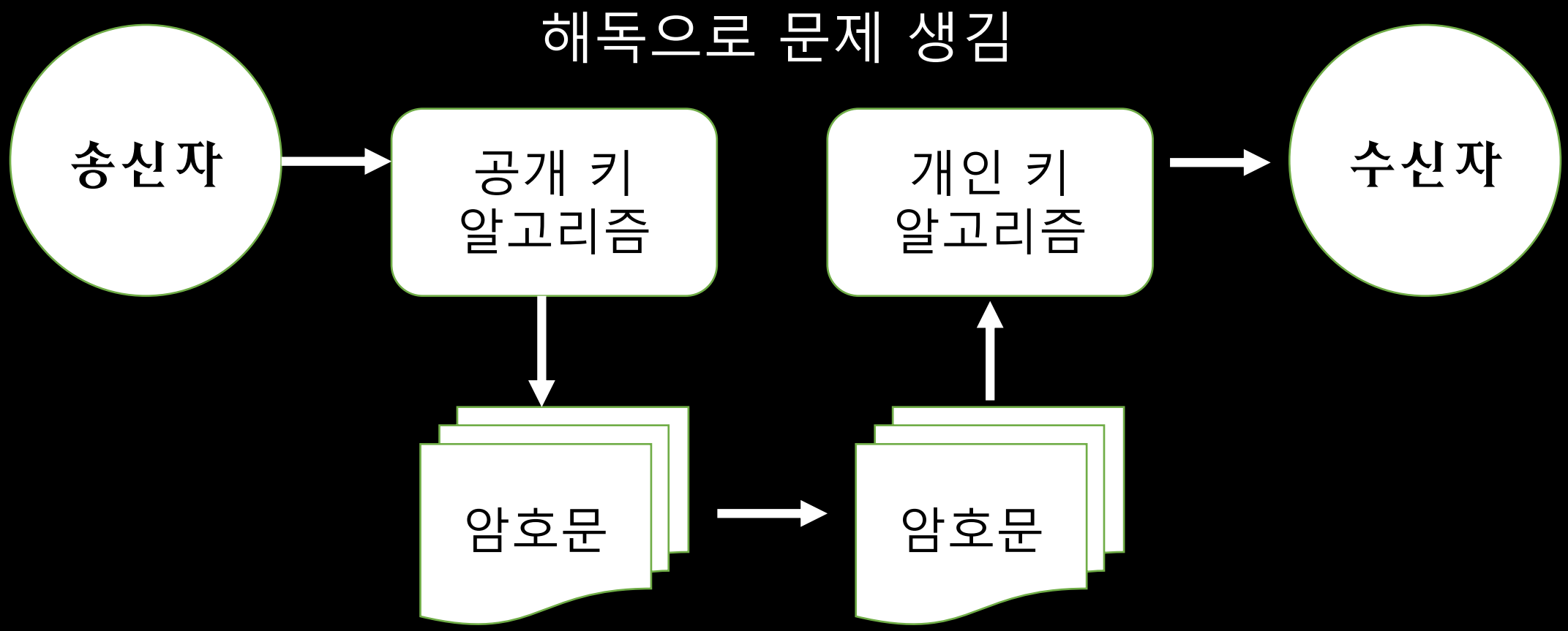
암호문

개인 키
알고리즘

암호문

수신자

문제점

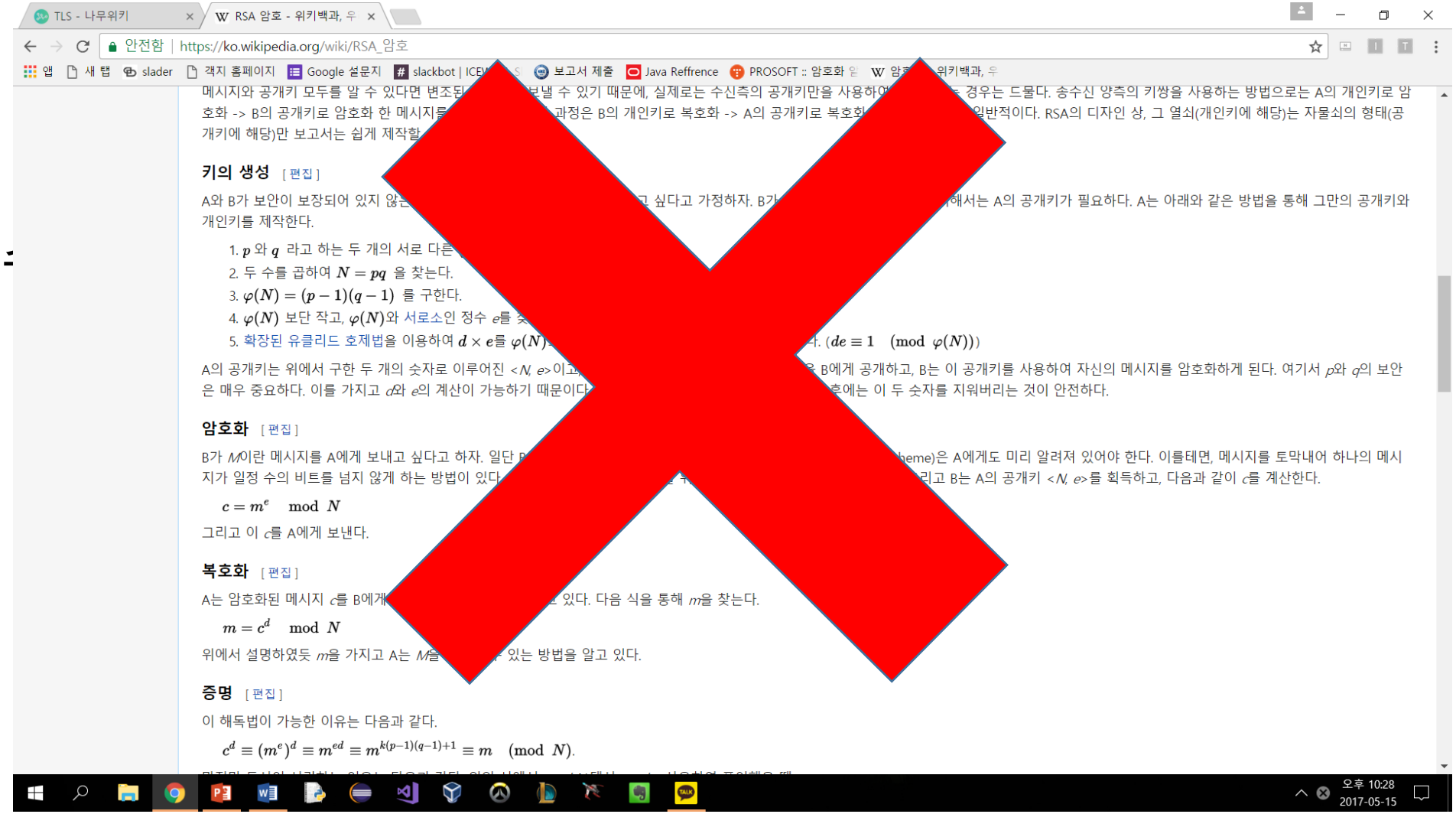


비대칭 KEY 종류

- RSA
- DSS

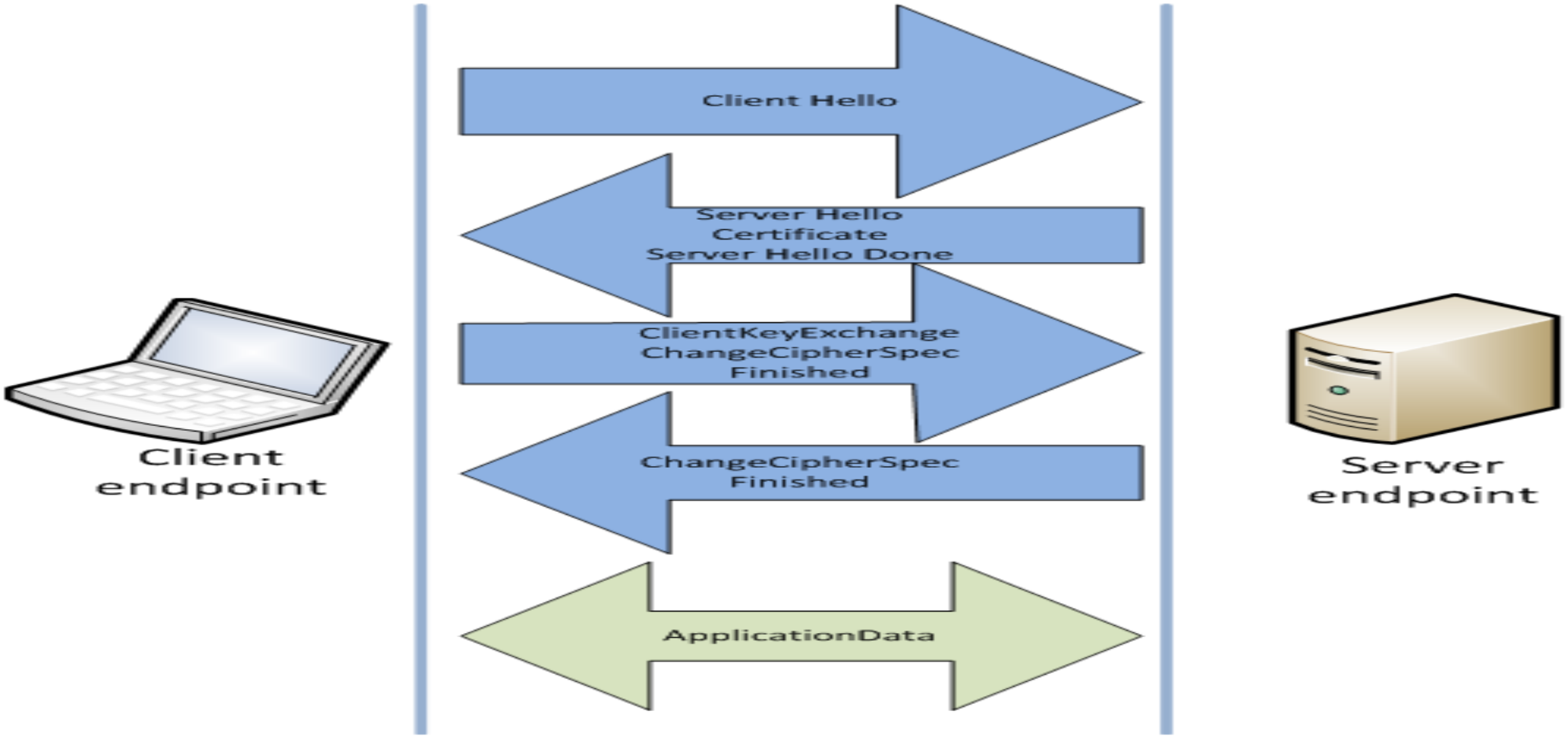
RSA (Rivest – Shamir - Adleman)

- 공개
- 소인




TLS

TLS (SSL)


Client Hello
Server Hello
Certificate
Server Hello Done
ClientKeyExchange
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished
ApplicationData
Client
endpoint
Server
endpoint

도와준 이

- 제갈지혜
- 이진명
- 기훈이 형

출처

- 수많은 나무위키, 위키백과 들
- 갓 구글링