RSA

Seoul National University of Science and Technology

Computer Science and Engineering

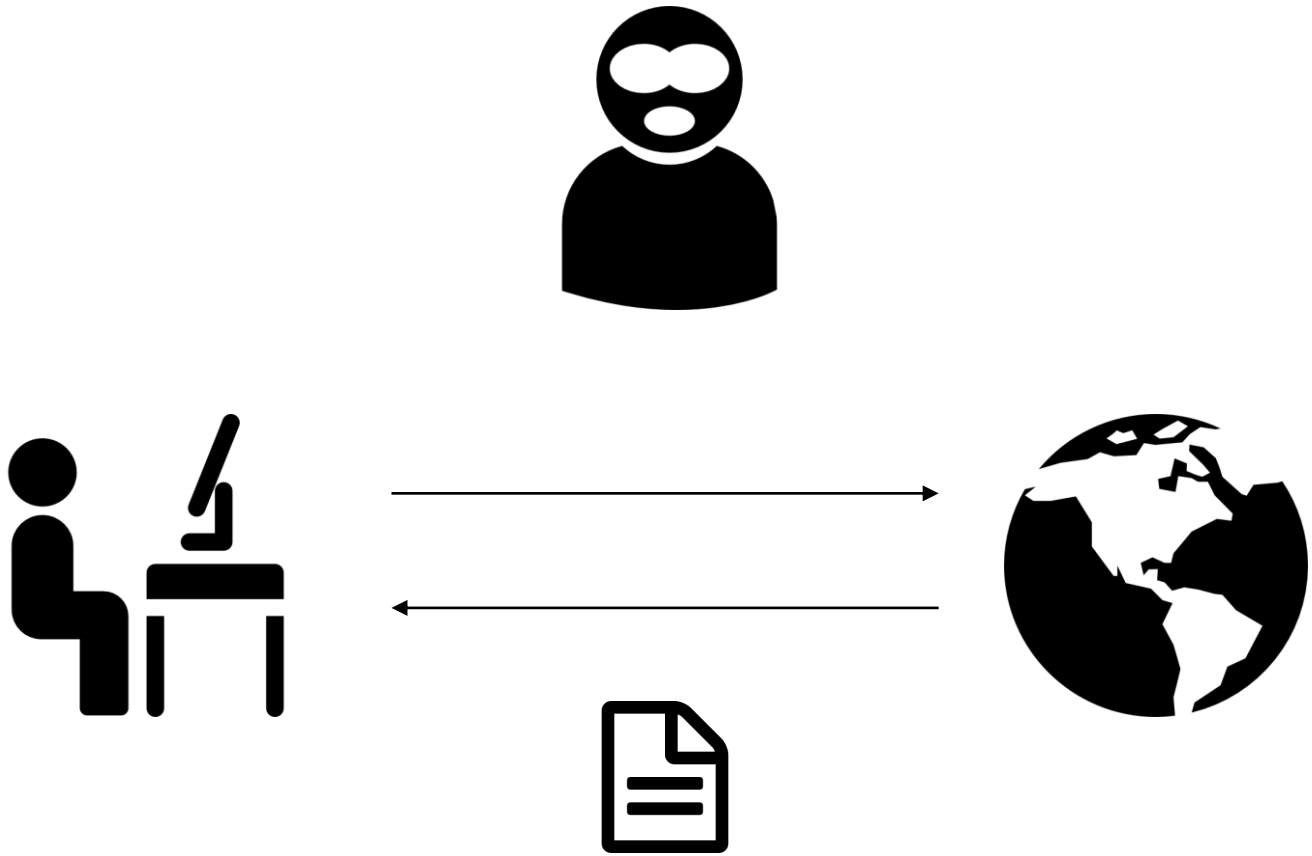
2019-05-23

STCIS
Seoul National University of Science and Technology
Cryptography and Information Security Laboratory

RSA Introduction

Network Environment

- 네트워크상의 모든 패킷 데이터는 공격자(Attacker)에게 노출될 수 있음
- 통신 과정에서 데이터를 보호하기 위해서는 암호화가 필요

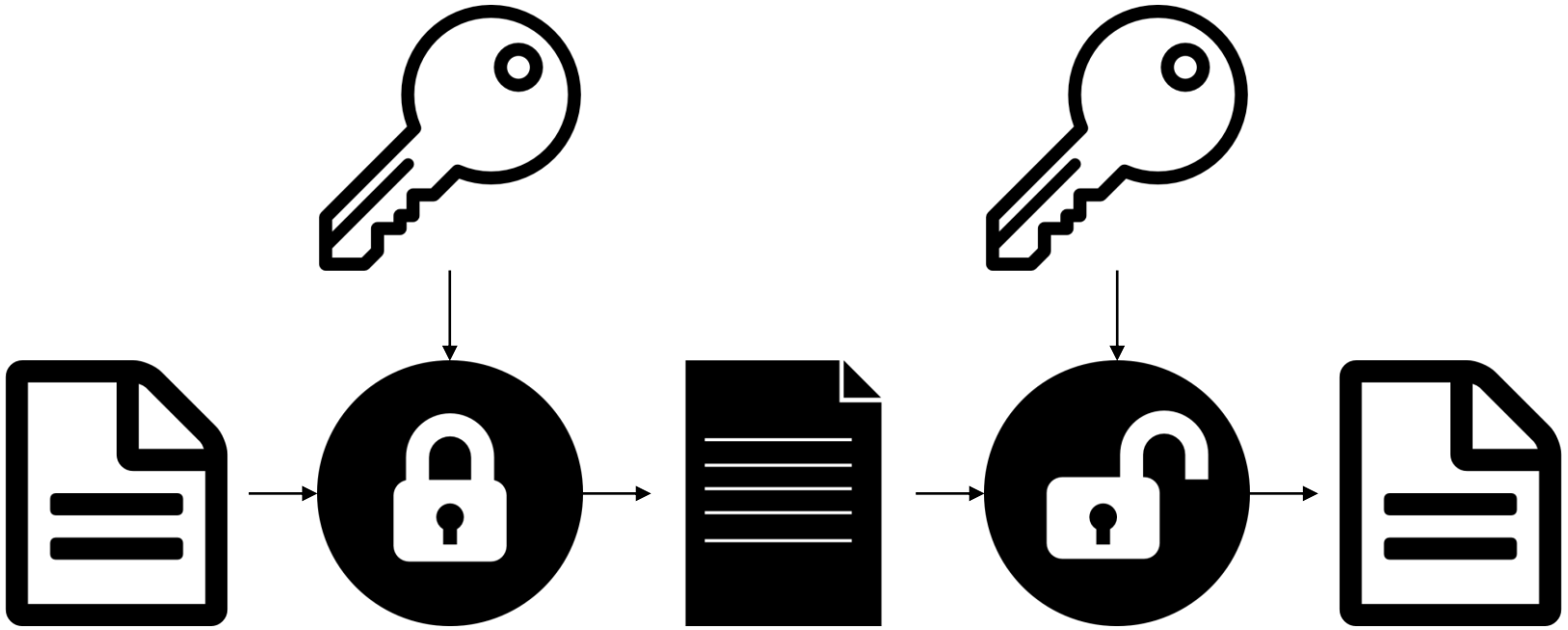


RSA Introduction

Block Cipher (= Symmetric Key Cryptosystem)

- 일반적인 데이터 암호화 알고리즘(AES, DES 등)을 수행하기 위해서는 두 통신 당사자끼리 미리 키(key)를 공유하고 있어야 함
- 키 정보 또한 상대방과 공유되는 과정에서 암호화된 상태로 전달되어야 함

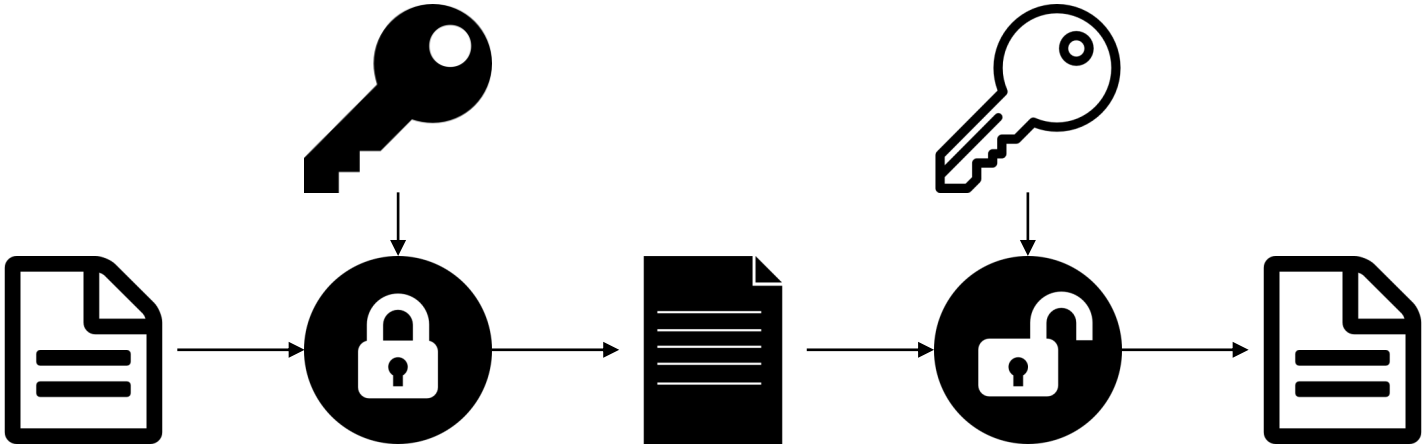
➢ 그렇다면, 처음으로 통신을 수행하고자 하는 두 대상이 최초의 키를 어떻게 공유할 것인가?



RSA Introduction

Public Key Cryptosystem (=Asymmetric Key Cryptosystem)

- 암호화 알고리즘과 복호화 알고리즘에서 서로 다른 키를 사용하는 공개키 암호(비대칭키 암호: RSA, ECC 등) 알고리즘을 이용
- 두 암호화 키 중 하나(Public Key)는 공개되어도 상관없음



RSA Algorithm

Key Generation

1. 서로다른 두 소수 p, q를 구한다.
   Find two prime number p, q $(p \neq q)$

2. $N = pq$ 를 구한다.
   Calculate $N = pq$

3. $\varphi(N) = (p-1)(q-1)$을 구한다.
   Calculate $\varphi(N) = (p-1)(q-1)$

4. φ(N)보단 작고, φ(N)와 서로소인 정수 e를 찾는다.
   Finds an integer e that is smaller than φ(N) and is prime to φ(N).

5. $d \times e$를 φ(N)로 나누었을 때 나머지가 1인 정수 d를 구한다. $(de \equiv 1\ (mod\ \varphi(N))$
   Find d $(where\ de \equiv 1 (mod\ \varphi(\mathrm{N}))$

- Public Key: $<N, e>$
- Private Key: $<N, d>$

1. $p = 61, q = 53$

2. $N = 61 \times 53 = 3233$

3. $\varphi(N) = (p-1)(q-1) = 60 \times 52 = 3120$

4. $e = 17$

5. $17 \times 1\ mod\ 3120 = 17,$
   $17 \times 2\ mod\ 3120 = 34,$
   $17 \times 3\ mod\ 3120 = 51,$
   ...
   ...
   $17 \times 2753\ mod\ 3120 = 46801\ mod\ 3120 = 1$

- Public Key: <3233, 17>
- Private Key: <3233, 2753>

RSA Algorithm

Encryption and Decryption

- Public Key: $<N, e>$
- Private Key: $<N, d>$

메시지 데이터(Plain text): p

암호화된 데이터(Cipher):

$$c = p^e \ mod \ N$$

복호화된 데이터(Plain text):

$$p = c^d \ mod \ N$$

- Public Key: <3233, 17>
- Private Key: <3233, 2753>

메시지 데이터(Plain text): 65

암호화된 데이터(Cipher):

$$c = 65^{17} \ mod \ 3233 = 2790$$

복호화된 데이터(Plain text):

$$p = 2790^{2753} \ mod \ 3233 = 65$$

Modulo

$$2790^8 \; mod \; 3233 = (3671416253212328096100000000) \; mod \; 3233$$

$$= (2790^2)^4 \; mod \; 3233 = (7784100)^4 \; mod \; 3233$$
$$= (7784100 \; mod \; 3233)^4 \; mod \; 3233$$
$$= (2269)^4 \; mod \; 3233$$
$$= (2269^2)^2 \; mod \; 3233$$
$$= (5148361 \; mod \; 3233)^2 \; mod \; 3233$$
$$= (1425)^2 \; mod \; 3233$$

Practice

Find the original plain text

$$p = 547$$

$$q = 593$$

$$e = 17$$

$$Cipher\ text = 132637$$

what is the Plain text?

Thank you