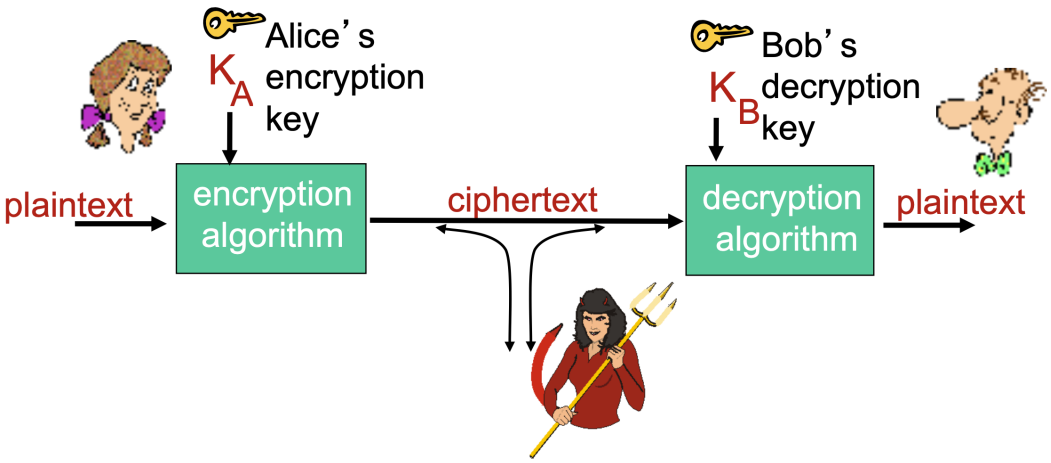
# 13일차

## Network Security

1. 정의
    a. 기밀성 : 허가된 사람만 접근 가능
    b. 무결성 : 허가된 사람만 정보를 변경 가능
    c. 가용성 : 언제든지 허가된 사람은 접근 가능
    d. authentication (인증)

2. The language of cryptography (암호학)




m plaintext message
$K_A(m)$ ciphertext, encrypted with key $K_A$
$m = K_B(K_A(m))$

    a. plaintext : 원문
    b. ciphertext : 암호문
    c. plaintext를 A가 가지고 있는 key 로 암호화(KA(m)) 후 B가 가지고 있는 key 로 복호화
    key는 같을 수 도 있고 다를 수 도 있다.

3. 암호화 공격방법 → 수업때 거의 넘어감

a. cipher-text only attack : 암호화문서를 가로챈 eve 는 암호화 알고리즘을 알고이를 plaintext로 바꿔서 plaintext를 만든다.

b. known-plaintext attack : eve는 plaintext와 ciphertext를 모두 알고 있다. 이를 통해 key를 유추한다.

c. chosen-plaintext attack : eve는 새로운 plaintext를 만들어 alice의 컴퓨터에 접근해 ciphertext를 만들어 낸다. 이를 분석하여 key를 유추한다.

d. chosen-ciphertext attack : eve는 가로챈 ciphertext의 일부를 이용해 새로운 ciphertext를 만들어 낸다. 이를 Bob에게 보내고 얻어낸 plaintext를 통해 key를 유추한다.

4. Symmetric key cryptography : 대칭키 암호화

a. 같은 key 값으로 암호화, 복호화함. → key를 공유하고 있어야함.

b. 대체 암호화

*substitution cipher:* substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
plaintext:  abcdefghijklmnopqrstuvwxyz
            |                       |
ciphertext: mnbvcxzasdfghjklpoiuytrewq
```

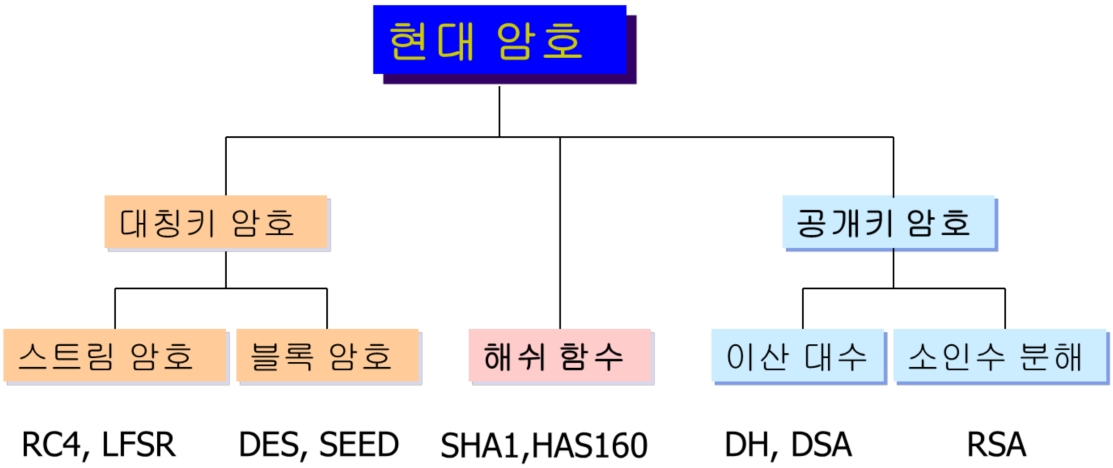
e.g.: `Plaintext: bob. i love you. alice`
`ciphertext: nkn. s gktc wky. mgsbc`

☞ *Encryption key:* mapping from set of 26 letters to set of 26 letters

1. a가 오면 m으로 바꿔주고 z가 오면 q로 바꿔주는 방식
2. cycling pattern : 1대1로 매칭하는 방식보다는 랜덤한 패턴을 가지고 도는 방식

- cycling pattern:
  - e.g., n=4: $M_1,M_3,M_4,M_3,M_2$; $M_1,M_3,M_4,M_3,M_2$; ..
- for each new plaintext symbol, use subsequent substitution pattern in cyclic pattern
  - dog: d from $M_1$, o from $M_3$, g from $M_4$

5. 현대 암호




a. 해쉬 함수 : 긴 문자열을 짧게 암호화

b. 대칭키 암호

   i. 스트림 암호

      i. 영상, 스트림 서비스에서 bit 마다 암호화

   ii. 블록 암호

      i. 블록 단위로 암호화 (DES가 대표적)

c. 공개키 암호 (비대칭키 암호)

   i. public, private키가 있음

   ii. 이산 대수 (DH, DSA)

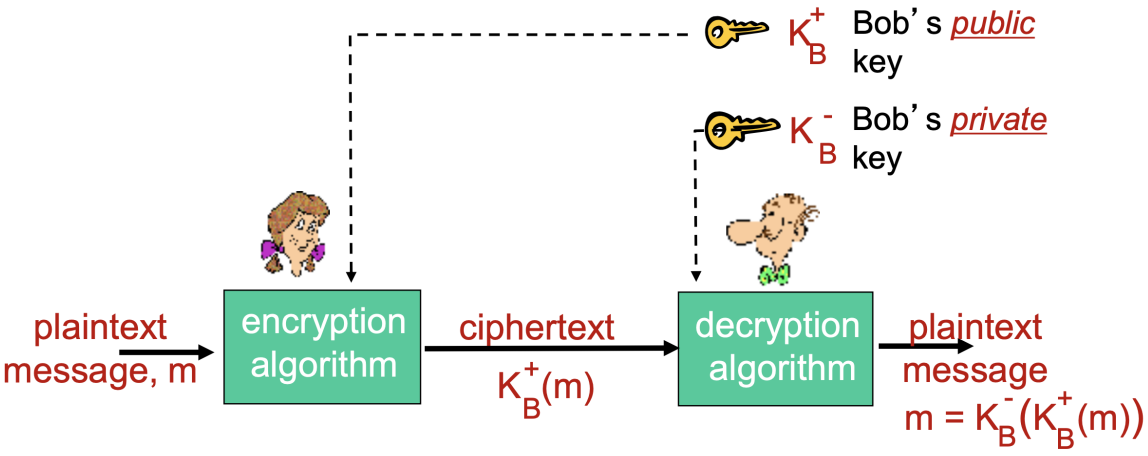
   iii. 소인수 분해 (RSA)

## Symmetric key Cryptography

1. DES (Data Encryption Standard)
    a. 56-bit symmetric key, 64-bit plaintext input
    b. 3DES : DES는 깨지기 쉽기 때문에 (컴퓨터 성능의 증가) 3개의 key를 쓴다.
2. AES (Advanced Encryption Standard)
    a. key 값 자체가 커짐(128, 192, 256)
    b. BES를 깨는데 1초가 걸린다면 AES는 149조 년이 걸림

## Public Key Cryptography

- Diffie-Hellman 방식을 기반
- secret key를 공유하지 않음
- public key는 모두 알고 private key는 받는 사람만 알고 있음.




public key로 암호화 한 후 private key로 복호화하는 방식

1 need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

2 given public key $K_B^+$, it should be impossible to compute private key $K_B^-$

*RSA:* Rivest, Shamir, Adelson algorithm

1. RSA
    a. 공개키 암호화 → private키 복호화 or private키 암호화 → 순서를 바꿔도 같은 결과
    b. 단점 : 느림

## Hash

- 임의의 길이를 갖는 데이터를 고정된 길의 데이터로 변환시켜주는 함수

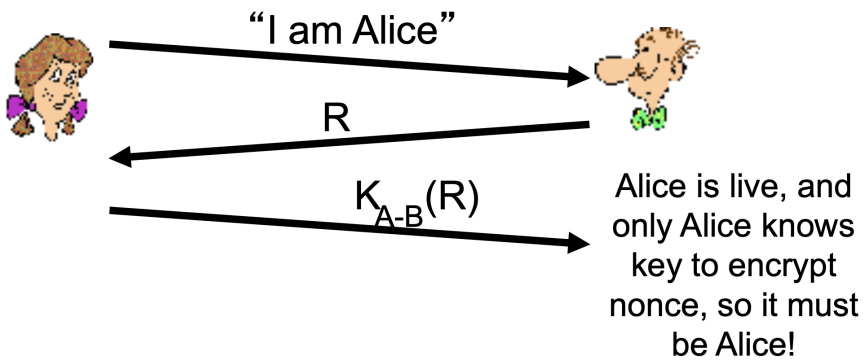
## Authentication

1. IP를 알려줌
2. IP, password를 알려줌
3. playback attack(재생공격) Alice가 Bob에게 보내주는 인증정보를 eve가 보내서 Alice인 척함
    a. 이를 피하기위해서 nonce 라는 일회성 숫자를 주고 암호화해서 받는 식으로 인증을 한다.

*Goal:* avoid playback attack

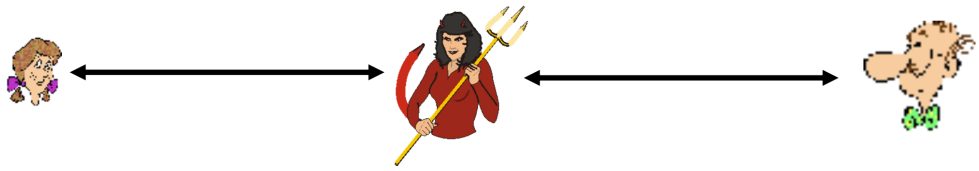
*nonce:* number (R) used only *once-in-a-lifetime*

*ap4.0:* to prove Alice "live", Bob sends Alice *nonce*, R. Alice must return R, encrypted with shared secret key




4. (공격) man in the middle attack
   a. 위의 방식도 man in the middle attack으로 인해 해커가 공격할 수 있다.

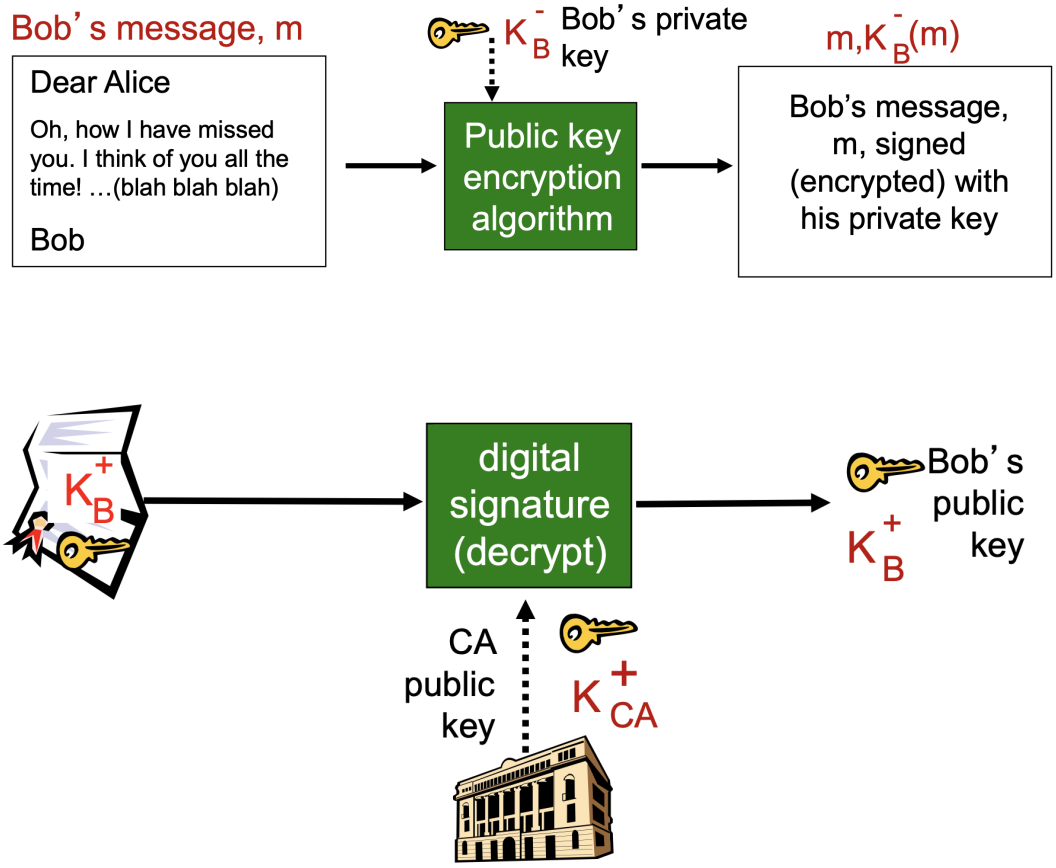
*man (or woman) in the middle attack:* Trudy poses as Alice (to Bob) and as Bob (to Alice)



difficult to detect:

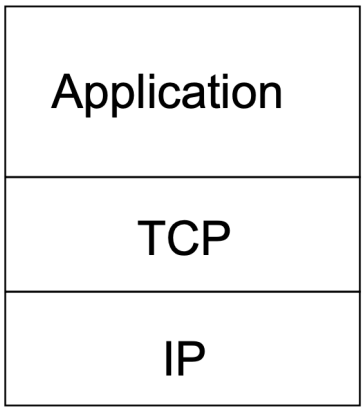
- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation!)
- problem is that Trudy receives all messages as well!

5. Digital signatures
   a. Bob이 원문과 원문을 본인의 private key로 암호화한 정보를 만든다.
   b. 그럼 공신력 있는 기관에서 public key를 통해 Bob이 보낸 건지 확인을 한다.

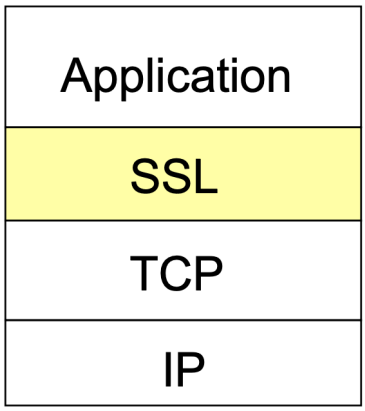



6. Secure e-mail
    a. 비대칭키 (공개키) + 대칭키 암호화 방식 모두 이용

## SSL : Secure Sockets Layer




*normal application*




*application with SSL*

1. Application 과 transport 사이에 넣음.

## IPsec protocols (네트워크 층 보안)

1. AH protocol : 인증, 무결성 O / 기밀성 x
2. ESP protocol : AH + 기밀성
3. VPN (Virtual Private Networks)
    a. 해외 등에서 회사 사설망에 접속하기 위한 사설통신망
4. IKE (Internet key exchange) → 대충 넘어감
    a. PSK : Pre Shared Key
    b. PKI : Public Key Infrastructure → 공개키기반

## WEP design goals

EAP

무선랜에서 암호화

1. 인증방식
    a. authentication request
    b. nonce

## Firewalls : 방화벽

- 망 자체로 들어 올때 방화벽을 두어 외부 공격을 막는다.
- IDS : 방화벽에 공격 detection (방화벽 만으로 다 막을 수 없음)