컴망 11주차 2차시

Alice bob 은 선의의 통신을 하는 애들

트루디 : bad guy

Encryption algorithm by key

* Ciphertext 를 제공

Bob 의 decryption key => plain text

이런 encryption scheme 에도 여러가지 어택이 존재 할 수 있음, 넘어감.

암호화에는 2가지

대칭키,

서로 간에 같은 암호화 정보를 알고 있다.

여러가지 Shared 알고리즘을 번갈아서 사용 할 수 있음. Cycling pattern

16 segment 로 나눠서 .permutation ?

Symmetric key crypto : DES( 표준 )

AES (Standard)

56bit key , 64 input plain txt. ~ (대충)

공개키/개인키

Sym : Send 와 receiver 가 shared 키를 가지고 있음. 어떻게 키에 agree 할 건가, share 할건가?

반대로 public/private 은 나한테 메시지 보낼 사람은 내 public, encryption 알고리즘으로 암호화 시켜서 보내라.

본인만 decryption 할 수 있다(private key).

RSA public 키를 알 때 , private 키를 알 수는 없어야 한다.

RSA 계산 하는 법 알아야 함.

Plain txt public 으로 encrypt 한 걸 private 키로 풀면 =m

Bob 의 private 로 encrypt 랑 public 으로 decrypt 해도 m 나옴

RSA 를 계산하는 거 보면 exponential 함수를 사용한다.

그렇기 때문에 DES( symmentic 알고리즘 ) 이 더 빠르다. =>긴 문장 rsa 적용은 어렵다.

Symm 을 사용해서 encrypt 했으면 key 에 대한 정보를 상대에게 알려줘야 함. 이 키에 대한 정보를 rsa 를 사용해서 암호화 시키는게 일반적. ( key 에 대한 정보는 짧거든)

Authentication

내가 00 이다 보냈을 때 과연 나를 증명 할 수 있을까?

Password 시스템 써도 듣고있다가(도청) 기록 해 놓고 고대로 사용 할 수 도 있어서 소용 x.

(play back attack), 저장 해 놨다가 나중에 사용.

Encrypt password 는?

이것도 똑같이 기록하면 되잖아..

참고 )그러면 encrypt 를 내 private key encrypt 를 사용하면?

Once in a life time (nonce)

Alice 야~ => bob 이 번호던짐(nonce) => alice 서로의 shared 키를 사용해서 encrypt 해서 보냄=>

Bob이 shared 키로 decrypt, R 이 맞으면 OK

근데 R 값은 그 당시에만 소용있는 번호 이기 때문에, play back attack 을 사용 할 수 없다.

Public private key 사용

Alice 만의 private key 로 encrypt

Man in the middle .공격은 막기 어려움 ( 이거 해결하기 위한 방법도 존재 ) 간단하게 이해만

Digital signature

Bob의 private key를 통해서 encryption 한

밥의 메시지와 encryption 한 거와 원래 메시지를 같이 보냄.

=>Bob 의 public key 를 사용해서 decryption

메시지가 같은지 확인

밥의 원래 메시지 크기가 매우클때는=>>메시지의 크기가 굉장히 클 때는?

Message digest 사용 => message 를 대상으로 hash func 사용해서 작은 메시지로 만듬.

Hash function algorithm 도 많다

128bit, 160 bit 로 줄어든다. 종류 알아놓기

여전히 man in the middle 을 막을 순 없다 .

Certification authority .

Public key를 인증서에 bind 한다.

.ex) bob의 public 키를 인증기관의 private 키를 bind 한다. => 그럼 인증기관의 public 키를 사용해서 풀기 => 여기서 인증 받은 키는 바로 쓸 수 있다.