Contents

Chapter 1

chapter 1 title

1.1 이동통신보안

1주차

암호화 기본 기법 네 가지. 이걸로 보안 시스템 구현 가능.

- 대칭키: $A : c = E(k, m)$, $A \to B : \mathsf{ID}(A), c$, $B : m = D(k, c)$. ID는 그 사람을 식별하기 위함. 공개키보다 빠르다. 블록 or 스트림 암호. 블록의 경우 운영모드가 있음. 전사공격 유일하게 허용. $O(2^n)$. AES, SEED, ARIA, LEA. 키 분배 문제. 확장성 문제(x명의 경우, $\binom{x}{2}$). 키 분배 문제: 키분배센터(KDC)라는 제 삼자 이용. KDC가 A와 B에게 k 전달. 커버러스 통신이 이거 사용.

$$\begin{aligned} &A \to C : \mathsf{ID}(A), \mathsf{ID}(B) \\ &C \to A : c_1 \leftarrow E_{k_{ac}}(k_{ab}), c_2 \leftarrow E_{k_{bc}}(k_{ab}) \\ &\qquad A : k_{ab} \leftarrow D_{k_{ac}}(c_1), c \leftarrow E_{k_{ab}}(m) \\ &A \to B : c, c_2 \\ &\qquad B : k_{ab} \leftarrow D_{k_{bc}}(c_2), m = D_{k_{ab}}(c). \end{aligned} \tag{1.1}$$

  이 과정의 문제점은, 키가 추가로 필요하다는 점. 추가로 필요한 키도 보호가 필요하다는 점. 이 문제를 공개키 암호가 해결할 수 있음.

- 공개키: 키가 두 개. 비밀키, 공개키. 둘은 수학적 연계. $B \to A : c = E_{pk_A}(m), A : m = D_{sk_A}(c)$. 내가 보냈음을 인증 가능. (인증, 부인방지. 공개키를 조작할 수 있나?) $B \to A : c = E_{sk_A}(m), A : m = D_{pk_A}(c)$. 이 둘을 합치면?

- 전자서명

- 해시

[1]

[1] 우리나라는 it 소비 강국. 해커의 공격이 많음.