- 보안 공격 : 조직에 의하여 정보의 안전성을 위태롭게 하는 제반행위
- 보안 기법 : 보안 공격을 탐지, 예방, 복구하기 위해 설계된 기법
- 보안서비스 : 조직의 데이터 처리 시스템 및 정보전송에 대한 안전성을 수행하기 위한 서비스

- 기밀성(가로채기) : 합법적인 실체만 읽을 수 있도록 보호하는 서비스
- 인증(위조) : 정보 및 시스템 자원을 사용하는 정당한 사용자임을 확인할 수 있도록 보호하는 서비스
- 무결성(불법 수정) : 합법적인 실체만 수정할 수 있도록 보호하는 서비스
- 부인봉쇄 : 송수신자가 송수신한 사실에 대한 부인을 하지 못하게 하는 것
- 접근제어 : 사용자가 시스템 혹은 특정 자원에 접근하고자 할 때 인가 받은 사용자만 접근을 허락하도록 제어하는 서비스
- 가용성(방해) : 컴퓨터 시스템이 인가 당사자만 필요로 할 때 이용할 수 있게 보호 하는 서비스

보안공격 대표적 4가지 유형

- 방해 : 시스템의 일부가 파괴되거나 사용할 수 없게 되는 경우로, 가용성에 대한 공격. (하드디스크 파괴, 통신회선 절단, 시스템 무력화)
- 가로채기 : 비인가자들의 불법적인 접근에 의하여 발생되는 기밀성에 대한 공격.
- 불법수정 : 비인가자들의 불법적인 접근 뿐만 아니라, 불법적인 변경에 의한 무결성에 대한 공격

적극적 공격	소극적 공격
전송 정보의 도청 / 감시 적의 목적 : 전송중인 정보를 취득 메시지 내용 공개 : 전화통화, E-mail, 전송파일 트래픽 분석 : 공격자가 암호 메시지의 유형을 보고 송수신자 신분, 통화시간 통신 성격 추측 탐지가 어렵기 때문에 탐지 보다는 예방에 촛점	신분위장 : 하나의 객체가 다른 객체의 행세를 할 때 발생(인증 순서를 알아내어 재전송하여 인증으로부터 특권 취득) 재 전송 : 데이터 단위를 수동적으로 획득→다시전송(비인가된 결과를 생성) 메시지 불법 수정 : 단순히 메시지 불법수정 순서지연(A→B가 읽을 것) 서비스 부인 : 특정 목표물을 무력화, 성능저하유발, 과다전송(서버공격) 예방보다는 탐지와 복구가 중요

전자문서와 종이문서의 다른점

종이 문서	전자 문서
원본과 복사본의 구별이 쉽다 변조되었을 때 물리적인 흔적이 남는다 (지우개로 지운 부분은 표면이 얇아지거나 거친 부분이 남게 된다) 원본 여부 판정(서명의 형성, 양각의 공증 철인)	비트열로 구성 원본과 복사본의 차이가 없음 원본여부는 문서자체에 포함된 정보만으로 판정. 문서에 물리적인 서명을 할 수 없음

관용암호 방식 장단점

장점	단점
→ 저가의 칩 → 알고리즘 수행속도 빠름 → DES,RC4,RC5,SEED,IDEA등 다양한 알고리즘 개발 → Key의 비밀성이 중요하기 때문에 저가의 다양한 알고리즘을 구현하고 개발	→ Key 관리가 어려움 → Key의 중요성 때문에 Key의 분배문제도 상당히 어려운 부분 → 디지털 서명이 어려움 → 인증에 대해서 약점을 지니고 있음

특징 : → 암호 알고리즘은 암호문 자체로만으로 해독 불가능
→ 안전성은 암호문 암호 알고리즘의 비밀성이 아니라 키의 비밀성에 의존
→ 암호문과 암복호 알고리즘이 알려져도 메시지의 해독이 불가능하다고 가정

- 치환 : 평문의 문자를 다른 문자나 숫자 또는 기호로 대체 시키는 방법
- 전치 : 평문자나 비트의 순서를 절차에 따라 위치를 재조정

절대 안전성 과 계산상 안전성

- 절대 안전성 : 비용과 시간이 충분하여도 복호하기가 불가능
- 계산상 안전성 : 암호 해독 시간이 정보의 유효 기간을 초과

스트림 암호 방식과 블록 암호 방식

- 스트림 암호 방식 : 한번에 1bit나 1byte씩 암호화(한문자)
- 블록 암호 : 연선을 블록 단위로 처리

확산과 혼돈

-확산 : 키를 추론하기 어렵게 하기 위해 평문과 암호문 사이에 통계적인 관계를 복잡하게 하는 것.

-혼돈 : 키를 발견하기 위해 암호문에 대한 통계 값과 암호키 사이의 관계를 가능한 복잡하게 만드는 것.

3중 DES사용 이유 : DES의 brute-force 공격에 대한 취약점을 보안하기 위해 사용
2키에 대한 3중 DES : 중간 결과의 의한 공격 대책 =>3단계 암호화 과정

$C_1=E_{K1}[D_{K2}[E_{K1}[p]]]$ $P=D_{K1}[K_{K2}[D_{K1}[P]]]$

3키에 대한 3중 DES : 168비트 효과적인 키 길이를 가짐

$C=E_{K3}[D_{K2}[E_{K1}[P]]]$

$P=D_{K1}[E_{K2}[D_{K3}[P]]$

▷ 3장 강의 자료 참고

블록암호 운영모드 5가지

운용 모드	암복호화 방식		응용	특징
ECB	E	$C_j=E_k[p_j]j=1, \ldots ,N$	짧은 자료 전송(예: 암호키)	
	D	$P_j=D_k[C_j]j=1, \ldots, N$		
CBC	E	$C_1=E_k[P_j \oplus IV]$ $C_j=E_k[P_j \oplus C_{j-1}]j=2,\ldots ,N$	범용 블록형 전송인증	
	D	$P_1=E_k[C_1] \oplus IV$ $P_j=E_k[C_j] \oplus C_{j-1}$ $j=2, \ldots, N$		
CFB	E		범용 스트림형 전송인증	
	D			
OFB	E		잡음있는 채널상의 스트림형 전송(예 :위성통신)	
	D			
CTR	E		일반용도의 블록형 전송 고속의 요구사항에 유용	
	D			

쇄도효과 : 암호 알고리즘의 바람직한 성질중의 하나, 평문이나 키의 작은 변호가 암호문에 대하여 중요한 변화를 일으키게 하는 것.

합동식의 계산 / 유클리드 알고리즘

링크 암호화 단대단 암호화 원리, 장단점

- 링크 암호화 : 암호화 장치를 통신 링크 양단에 모두 설치
- 단대단 암호화 : 암호화 과정을 두 종단 시스템에서 수행(동일한 키 공유)

	링크 암호화	단대단 암호화
장점	모든 링크상의 모든 트래픽 보호	전송로와 교환기 내에서 데이터 보호 간단한 인증 기능 제공 링크 암호화보다 적은 Key
단점	패킷교환기내에서 Data, Header노출 링크간에 많은 암호화장치 필요 공유해야 할 키가 증가(2key필요)	전송로와 교환기내에서 헤더 노출 트래픽 패턴은 안전하지 않음

(1) 암호화를 수행할 때 필요한 비밀 키의 개수 : [N(N-1)/2]-세션키 N-마스터키
(2) 키 분배 센터를 통하여 키 분배 :
→ 단대단 암호화에서 널리 채택
→ 사용자는 키 분배 센터와 유일한 키 공유
→ 제 3자의 신뢰 문제, 3자와의 공증 효과
(3) 키 분배 시나리오
1. A는 C에게 B와의 통신을 위해 세션키를 요구
Request||N1 → 난수를 비표로 사용
2. C는 A에게 $E_{Ka}[K_S||Request||N_1||E_{Kb}(Ks, ID_A)]$
3. A는 $E_{kb}(K_S , ID_A)$를 B에게 보낸다
4. B는 $E_{KS}[N_2]$를 A에게 보낸다
5. A는 N_2를 얻어 $E_{KS}[f(N_2)]$를 B에게 보낸다

시이저 암호방식 :
→ 합동식 : mod n
→ 쥴리어스 시저에 의해 개발
→ 암호문 : C = E(P) = (P+3) mod (26)
복호문 : P = D(CP = (C-3) mod (26)

Vernam 암호방식 :
→ 통계적 해독을 방지하기 위해 키워드를 평문과 같은 길이로 사용
→ Ci = Pi ⊕ Ki
Pi = 평문의 i번째 비트, Ki=키의 i번째 비트, Ci = 암호문의 i 번째 비트
→ Pi = Ci ⊕ Ki

Vigenere 암호방식 :
→ 평문자에 대한 암호 문자가 유이한 키워드의 각문자에 대하여 여러개 존재
→ 키워드를 필요한 만큼 반복적으로 사용

One-Time-Pad :
→ 실질적인 문제는 송수신자가 모두 이 랜덤키를 보유하고 보호
→ 사용이 어려운 이유 : 다량의 랜덤키 생성/관리가 어려움 , 키의 분배과 보호가 어려움

XOR암호 방식 :