정보보호론 0325

고전 암호

비제네르 암호

특정 길이의 키워드를 비밀키로 사용

하나의 문자가 여러 개의 문자로 치환

L = 키의 길이( 고정 x )

평문과 키워드가 매칭이 되는 경우

운이 좋게 평문과 키워드가 매칭 되는 경우

키 길이를 확인한 후 같은 키 자리 문자들을 모아서 빈도수 측정

전치 암호

위치를 변경하는 암호

현대 암호

블록암호

평문을 블록 단위로 64비트로 일정하게 나눠서 각 단위마다 암호화를 수행

스트림 암호

유연하게 비트 단위로 암호화를 수행

평문 + XOR 연산

메시지 부호화

부호화(encoding)

* 문자열을 디지털 기기에서 인식할 수 있도록 비트 (0 or 1)로 대응
* 정해진 방법대로 부호화 한다
* 키가 없기 때문에 encryption(암호화)가 아니다.
* 기밀성이 제공되지 않는다.

Ex) ASCII 코드

배타적 논리합

* XOR(eXclusive OR) 연산자
* 2개의 입력 비트가 같으면 0, 다르면 1
* 자기 자신을 연산하면 모두 0
* 자리수가 같아야 연산이 가능하다
* canceling : 없어진다는 의미

블록 암호 설계 기본 원리

혼돈 : 치환 개념(치환 -> 혼돈)

* 암호문과 비밀키의 관계를 난해하게 만든다
* 키와 암호문 관계를 감춘다.
* 키의 여러 부분으로 암호문이 생성된다.

확산 : 전치 개념(전치 -> 확산)

* 평문에 1비트가 변경되면 암호문에 절반 정도가 변경되어야 확산이다.

블록 암호 설계 기본 구조

곱 암호 구조

* 혼돈 + 확산
* 라운드 : 특정 부분이 여러 번 반복되는 구조
* SPN구조, Feistel 구조

페이스텔 구조

1라운드

* 암호화와 복호화 과정이 같다
* 암호화 알고리즘과 복호화 알고리즘을 따로 구현할 필요가 없으므로 구현이 용이하다
* 비가역 요소(가역 : 역으로 오는 것이 가능한 것)
* 왼쪽만 작업

다중

* 왼쪽과 오른쪽을 교차

2라운드

* 오른쪽만 작업
* 따라서 1번 작업할 때, 최소 2라운드까지는 작업해야한다.
* 라운드마다 key가 다르다.

DES(Data Encryption Standard) 탄생 배경

NIST의 대칭키 암호에 대한 표준 알고리즘 공모(1973)

IBM Lucifer를 수정하여 DES로 선정(1977)

NAS의 수정된 버전

S-Box 형태 변경(설계 원리 비공개)

AES로 대체되며 DES표준 공식 철회(2005)

DES 기술 개요

* 64비트 평문 데이터 블록을 처리하여 64비트 암호문 출력
* 비밀키는 56비트(2의 56승) = 56비트 안정성
* 현재 128~256비트 안정성이 적당함(2의 128승\_번~ 2의 256승\_번)
* 초기 순열(전치), 키 스케줄링 함수, 최종 순열, 16라운드 페이스텔 구조