정보보호론 0327

키 스케줄링

* 64비트 비밀키 입력
  + 56비트 : 비밀키
  + 8비트 : 에러 체크
* 16개의 48비트 라운드키 출력
* 16라운드 중 14번 정도 사용되도록 설계

초기 순열과 최종 순열

* 초기 순열과 최종 순열은 역관계에 있다.
* 자리 바꿈이 일어난다

페이스텔 구조의 F함수

* F(R\_i-1, K\_i)
* 32비트 값 출력

전사적 공격(brute force attack)

* 무차별적으로 공격 방법
* DES에 특화된 공격

차분 분석(differential cryptanalysis)

* XOR의 차
* 선택 평문 공격 (CPA)
* 두 평문의 차분과 암호문의 차분의 관계를 분석
* 2^47개의 평문/암호문 쌍을 가지고 2^47의 계산량으로 비밀 키 추측 가능

선형 분석(linear cryptanalysis)

* 알려진 평문 공격(KPA)
* 2^43의 평문/암호화 쌍을 얻을 수 있다며 높은 확률로 선형 표현식을 얻음

2중 DES (Double DES)

* 서로 다른 2개를 키 이용하여 DES를 두 번 사용
* C = Enc\_k2(Enc\_k1(m))
* 57비트 안전성 제공(DES는 56비트 안전성)
* 2 \* 2^56 = 2^57
* 의미가 없다.

3중 DES

* 기존 DES를 3번 사용
* 1. E -> D -> E
* 2. D -> E -> D
* E -> E -> E 사용하지 않는 이유는 구현 용이하기 위함
* 2^112
* 현재 사용 중지
* 과거 암호 복호화 하기 위해 알고리즘 공개

AES(Advanced Encryption Standard)

* 90년대 DES는 더 이상 안전하지 않음
* 하드웨어 성장이 빠르기 때문에
* TDES(Triple DES)의 약점
  + 속도가 느리다
  + 안전성 비효율적
  + 확장하기 어려움
* 양자컴퓨터는 비트를 반으로 나눈다, 그러므로 대칭키의 키 길이를 2배로 늘려주면 안전하다
* 양자컴퓨터 환경에서 비밀키는 적어도 256비트 크기가 바람직함
* NIST의 AES 공모
  + 요구사항
    - 128, 192, 256비트 중 하나로 사용
    - 소프트웨어 하드웨어 모두 효율적 구현

AES 기술 개요

* 비페이스텔 구조
  + 역방향이 존재하는 가역 요소
* 128비트 암호문 출력
* 3종류 : 128, 192, 256 비트
* AES 암/복호화 알고리즘 구성
* N라운드( 10, 12, 14) : 비밀키의 크기로 결정
  + subByte, ShiftRow, MixColumn, AddRoundKey
* 키 확장 함수
  + RotWord, SubWord, RCons

AES 128비트 블록 표현 방법

* 4 x 4행렬 : 상태
* 128bit = 16bytes

라운드 구성

* SubByte