암호학

암호 알고리즘

DES(Delta Encryption Standard)

* 64비트 블록암호 * 키의 길이가 56비트 * 16라운드를 반복 * 복호화는 암호화 과정과 같고, 키의 적용만 거꾸로 한다.

SEED

* 전체적인 구조는 Feistel 구조로 이루어져있다. * 블록길이만 다를 뿐 DES 구조와 같다. * 1998년 KISA가 초안을 개발하여 1999년 2월에 국내 블록암호 표준안을 제안했다.

타원곡선암호(Elliptic Curve Cryptography)

* 타원곡선상의 이산대수 문제를 제안한 암호시스템으로 RSA 알고리즘보다 작은 비트수를 가지고 동일한 암호강도를 지닐 수 있다. * 스마트카드나 휴대폰 기기 등 키길이가 제한적인 무선 환경이나 작은 메모리를 가지고 있는 시스템에 적합

SHA (Secure Hash Algorithm)

* 1993년 미국 NIST에서 개발 * 미국표준 FIPS PUB 180으로 공포되었고, 160비트의 해쉬코드를 출력 * MD4 알고리즘에 기반을 둔 해쉬함수

해쉬함수

조건

* 압축 (Compression)

- 가변의 길이 입력값으로부터 고저으이 길이 출력값을 생성

* 일방향성(One-Wayness)

- 특정 값에서 구한 압축된 출력값이 주어졌을 때, 해당 출력값으로부터 입력값을 역계산하는 것은 계산상 불가능해야 함

* 충돌회피(Collision Free)

- h(M1) = h(M2) 인 서로 다른 M1과 M2를 구하기는 계산상 불가능해야 함

* 효율성(Efficience)

- M으로부터 h(M)을 구하는데 많은 자원과 노력이 소요되지 않아야 함

생일 역설(Birthday Paradox)

특정 장소에 23명 이상 모이면 그 장소에 생일이 동일한 사람들 한쌍이 존재할 확률은 1/2 이상이다.

대칭키 암호시스템

스트림 암호시스템

* 암호화에 적용되는 평문의 길이에 따라서 난수열을 생성하여 입력. * 평문 비트열을 한 비트 또는 한 문자 단위로 XOR하여 암호화

블록 암호시스템

* 입력 평문 비트열을 일정한 크기의 블록으로 나누어 암호화

혼돈

* 평문의 작은 변화가 암호무넹 어떤 변화를 일으킬 것인지 예측할 수 없는 성질 * 암호문과 키 사이의 관계를 숨김 * 비선형 함수

확산

* 평문을 구성하는 각각의 비트들의 정보가 여러 개의 암호문 비트들에 분산되는 성질 * 전치와 치환을 통해 암호문과 평문의 관계를 숨김 * 선형 함수

Feistel 구조

* 블록암호 * 평문 두 개를 블록으로 나누어 배타적 논리합과 스왑을 이용한 라운드를 가짐 * 혼돈과 확산 이론을 가짐 * 라운드 수는 단일과정으로는 보안성이 부족하지만 라운드 수를 증가시키면서 여러 번 수행하면 보안을 강화 * 전형적인 라운드 수는 16라운드를 거친다.

공개키(비대칭키) 암호시스템

대칭키, 공개키(비대칭키) 비교

구분	대칭키 암호시스템	공개키(비대칭키) 암호시스템
장점	* 키 크기가 상대적으로 작다. * 암호 알고리즘 내부구조가 단단하여 시스템 개발 환경에 용이하다 * 각 암호시스템에 기초적으로 작용한다. * 암 · 복호화 속도가 빠르다.	* 대칭키 암호시스템보다 키분배가 용이하다 * 대칭키 암호시스템보다 확장성이 좋다 * 인증과 부인방지가 가능하다 * 범용적으로 사용이 가능하다

구분	대칭키 암호시스템	공개키(비대칭키) 암호시스템
단점	* 키 교환 당사자 간에 동일키를 공유해야 하므로 키 관리에 어려움이 있다. * 자주 키 교환을 해야 하므로 불편한다 * 디지털서명 등의 기법에 적용하기 곤란하다. * 중재자가 필요하다	* 대칭키 암호시스템보다 키 길이가 크다 * 암호화 처리 시간이 길다 * 공개키 배포의 신뢰성에 문제가 있다 * 복잡한 공개키 관리 구조를 필요로 한다
예	DES, 3DES, IDEA, AES, SEED, ARIA 등	RSA, ECC, Schnorr, Diffie-Hellman, DSA, KCDSA 등

관련 문서

Plugin Backlinks: 아무 것도 없습니다.