

과정명	
13차시	암호 연구 개발 기획

<1> 암호 알고리즘

[1] 암호 알고리즘 정의

- 정보 보호에서 암호(Cryptography)는 중요 정보를 다른 사람들이 해석할 수 없게 하는 방법 즉, 외부로 정보가 노출되는 것을 보호하기 위해 그 내용을 변경하는 방법을 뜻함
- 암호화 과정에서 핵심요소는 암호화 알고리즘과 키
- 암호 알고리즘은 평문을 암호문으로 변환하고 암호문을 다시 평문으로 변환할 때 사용하는 알고리즘 넓게 보면 암호 기술에 사용되는 모든 알고리즘을 뜻함
- 자료의 디지털화(化)가 급속도로 진행 되며, 네트워크를 통한 자료의 전송이 증가하고 이로 인해, 해킹 등을 통한 자료의 유출이 발생되었는데, 유출된 디지털 자료는 빠르게 유포되어 피해가 커지고 회수가 어렵기 때문에 암호화가 필요해짐
- 암호를 사용하면 정보와 시스템을 보호할 수 있음
- 암호 관련 용어

평문	송신자와 수신자 사이 주고받고자 하는 내용을 적은 일반적인 문장
암호문	암호화의 대상이 되는 문장으로 한글이나 영어 등의 일반 언어로 작성된 문장
암호문	송신자와 수신자 사이에 주고받고자 하는 내용을 제3자가 이해할 수 없는 형태로 변형한 문장
암호화	평문을 제3자가 알 수 없도록 암호문으로 변형하는 과정
복호화	암호문을 다시 일반인들이 이해할 수 있는 평문으로 변환하는 과정
암호 알고리즘	암호화와 복호화에 사용되는 수학적인 함수
키	평문의 암호화 과정이나 암호문의 복호화 과정에 필요로 하는 파라미터
송신자	평문을 암호문으로 변경하여 수신자에게 전달하는 사람
수신자	암호문으로부터 평문을 복호화하는 사람
암호해독(암호공격)	암호 방식의 정당한 사용자가 아닌 제3자가 불법적으로 암호문으로부터 평문을 원상 복구하는 시도

[2] 암호 알고리즘의 분류와 암호화 기술

- 암호 알고리즘은 크게 양방향과 단방향으로 분류됨
- (1) 양방향 알고리즘
 - 암호화된 암호화문의 복호화가 가능한 알고리즘으로 대칭키, 비대칭키 방식으로 분류
 - 1) 대칭키 방식
 - 사용하는 키와 복호화 할 때 사용하는 키가 동일함
 - 주로 파이스텔 네트워크, S-Box를 통해 블록 암호로 만들어지며 AES, DES 등이 이에 해당함
 - 키를 안전하게 전달할 방법이 없다는 단점이 존재함
 - 블록 암호 알고리즘과 스트림 암호 알고리즘으로 분류

블록 암호 알고리즘	암 · 복호화 연산 수행에서 2비트 이상의 고정된 크기의 블록 단위로 변환하는 방식 임의 길이의 평문을 암호화 시키기 위해서는 평문을 특정한 길이의 블록으로 분할하고 암호화 알고리즘을 적용하여 암호화한 블록 암호에 입력 전치와 치환을 반복하여 키에 대한 안정성을 보임 Feistel 구조의 DES, 3DES와 SPN 구조인 AES, IDEA
스트림 암호 알고리즘	이진화된 평문 스트림과 이진 키 스트림을 비트 단위로 XOR 연산하여

	암호문 생성 XOR을 사용하여 쉽게 일반 텍스트로 되돌릴 수 있는 가역성을 보유 OPT, RC4
--	---

2) 비대칭키 방식

- 하나의 키 쌍이 존재하는 알고리즘으로 두 개의 키 중 하나는 반드시 공개되어야 통상적인 사용이 가능함.
- 키 배송에는 문제가 없으나 대칭키 암호에 비해 현저하게 느리기 때문에 일반적으로 비대칭형 암호를 이용한 대칭키 암호 배송과 실제 암호문의 대칭형 암호 사용으로 상호보완적으로 이용
- 수학적 개념에 따라 인수분해, 이산대수, 타원곡선 방식으로 분류. 인수분해 기반 방식으로는 RSA, Rabin이 있고 이산대수 방식으로는 Diffie-Hellman, Elgamal, Schnorr가 있으며 타원곡선 방식으로는 ECC가 있음

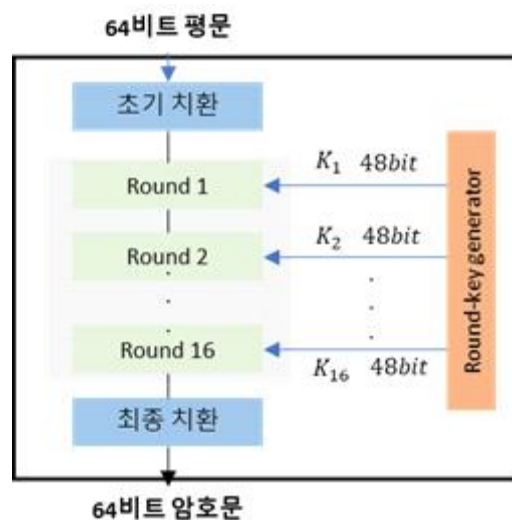
(2) 단방향 알고리즘

- 평문의 암호화는 가능하나 암호문을 평문으로 복호화하는 것이 불가능함
- Hash 알고리즘이 이에 해당하며 SHA와 MD 기술 등이 Hash 알고리즘을 사용

- 암호화 기술 종류

(1) DES

- 미국 NIST에 의해 미국 연방 정보에 사용되던 표준 암호로 가장 대표적인 대칭 암호화 방식
- 64비트 평문을 64비트 암호문으로 암호화하며 64비트보다 큰 평문의 암호화는 평문을 64비트로 나눠서 암호화
- 컴퓨터 성능 발전과 함께 현재는 전사 공격으로 DES 암호 해독이 가능함. 1998년 11월 이후 DES 암호는 공식적으로 사용중단 선언됐기 때문에 현재는 완전한 암호 방식이 아님



(2) 3DES

- DES의 대안으로 제시된 암호 알고리즘으로 DES를 3번 연속 실행하는 것이 기본 개념
- DES 알고리즘의 2배 정도의 암호화 강도이나 안전을 보장할 수준은 아님

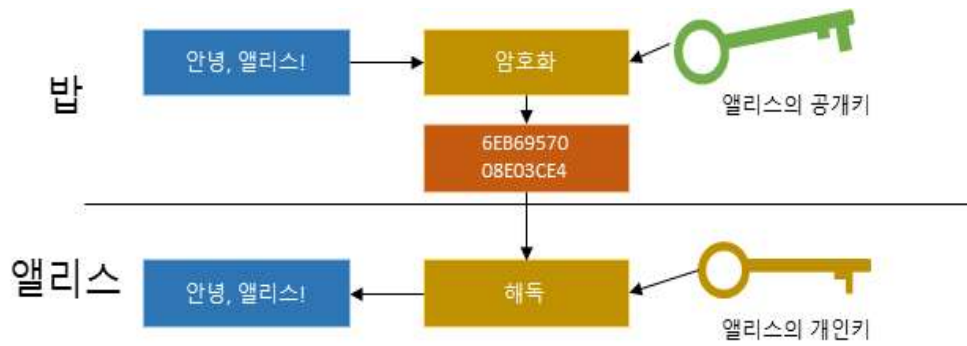
(3) AES

- 1997년 미국 NIST의 암호 공모에서 채택된 암호로 DES를 대체하는 미국 표준 대칭키 알고리즘
- 하드웨어 적용이 가능한 효율적인 알고리즘이며 메모리를 적게 사용하고 속도가 빨라 모바일 장비에서 사용하기 유리함
- 128비트 평문을 128비트 암호문으로 암호화하며, 키의 크기는 128, 192, 256으로 설정 가능

(4) RSA

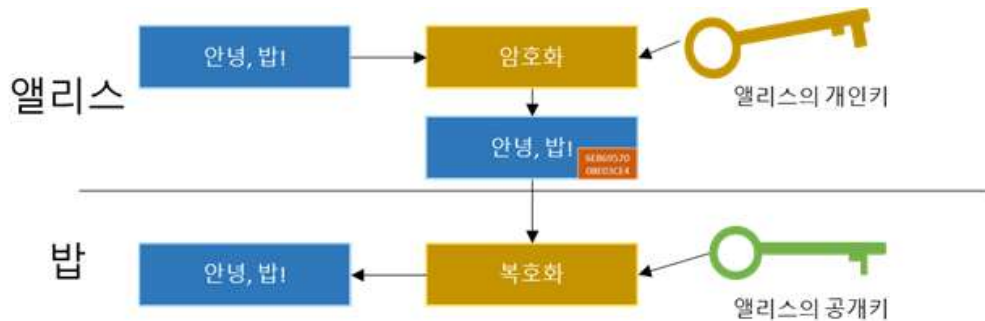
- 비대칭 알고리즘에 기반을 둔 암호화 방식으로 공개키와 개인키가 존재함

1) 공개키 암호화, 개인키 복호화



- RSA에서 사용되는 가장 대표적인 시나리오
- 대칭키의 배포가 필요 없이 미리 알려진 공개키 획득으로 키 교환 없이 암호화가 가능하여 다른 사람이 중간에 도청할 수 없는 기밀성이라는 특징을 갖게 함

2) 개인키 암호화, 공개키 복호화



- 자신이 서명한 사실을 부인할 수 없게 하는 부인 방지라는 특징을 갖게 됨

(5) 타원 곡선 암호(ECC)

- RSA에 비해 키의 크기가 작고 높은 보안성 제공이 가능한 비대칭 암호화 방식
- RSA보다 암호화 및 복호화 속도가 빠르며 자원 효율성이 높아 스마트 카드, 휴대전화 등의 작은 하드웨어에서도 잘 작동함

<2> 암호의 역사

[1] 고대 암호와 근대 암호

(1) 고대 암호

- 암호는 고대 그리스 시절부터 주로 군사나 정치적 목적으로 사용함
- 고대 암호의 종류로는 전치 암호, 치환 암호, 합성 암호 등이 있음
 - 1) 전치 암호는 $n \times m$ 개의 문자열을 m 개씩 끊어서 $n \times m$ 행렬을 만들어 세로로 읽는 암호화 방식임
 - 2) 치환 암호는 메시지의 각 문자의 위치 변화 없이 문자 자체를 다른 형태의 요소로 대체시켜 암호화하고 역처리시켜 복원하는 방식임
 - 3) 합성암호는 전치암호와 치환 암호를 적당히 조합시킨 방식임

(2) 근대 암호

- 17세기 근대 수학의 발전과 더불어 고급 암호가 발전하기 시작하였으며, 대표적으로는 Vigenere가 고안한 복수 시저 암호와 Playfair의 2문자 조합 암호가 있음
- 20세기에 들어서는 통신 기술의 발전과 기계식 계산기에 대한 연구를 바탕으로 두 차례의 세계 대전을 통한 암호 설계와 해독의 필요성이 높아지면서 암호에 대한 연구가 활발히 진행됨
- 20세기 근대 암호의 이론적 기초가 된 인물로는 프리드만과 새넌이 있음
 - 1) 프리드만은 1920년 '일치 반복률과 암호 응용'이라는 논문을 썼으며, 독일군이 사용하던 에니그마 암호와 일본군이 사용하던 무라사키 암호를 해독함
 - 2) 새넌은 1949년 '비밀 시스템의 통신 이론'이라는 논문을 발표했는데,

여기서 일회성 암호 체계의 안전함을 증명하고 암호 체계 설계의 두 가지 기본 원칙인 '혼돈과 확산 이론'을 제시 함

[2] 현대 암호와 차세대 암호

(1) 현대 암호

- 현대 암호는 1970년대 후반 스탠퍼드 대학과 MIT 대학에서 시작됨
- 1976년 스탠퍼드 대학의 Diffie와 Hellman이 '암호의 새로운 방향'이라는 논문에서 처음으로 공개키 암호의 개념을 발표했고, 1978년 MIT 대학에서 소인수분해 문제에 기반을 둔 RSA 공개키 암호를 개발하였고, 공개키 암호의 도입은 현대 암호의 발전에 중요한 계기로 작용함
- 1977년 미국 상무성 표준국이 DES 표준 암호 알고리즘을 채택하였고, DES 표준화를 계기로 금융 시스템을 중심으로 상업용 암호화의 이용이 증가하고 컴퓨터 통신망을 이용한 문서 전송, 전자 자금 이체 등이 활성화되었으며 암호 방식이 일반인들에게 알려지고 널리 사용됨
- 이전 암호 방식은 키, 암호 알고리즘을 비밀로 했지만 현대 암호에서는 알고리즘을 공개하고 있음

(2) 차세대 암호

- 양자 기반 알고리즘인 Shor 알고리즘은 인수분해 문제의 해결 속도를 감소시켜 RSA, ECC 등 인수분해 및 이산대수 기반의 공개키 암호 알고리즘의 더 이상 사용할 수 없게 함
- Grover 알고리즘은 정렬되지 않은 데이터베이스의 원소를 검색하는 속도를 향상시켜 대칭키 암호는 키 사이즈를 2배, 해시 함수의 출력 길이를 3배 증가시켜야 기존의 안정성을 가질 수 있게 됨
- 특정 상황에서 기존 현대 암호기술이 해결하지 못하는 경우를 대비하여, 새로운 암호기술에 대한 연구가 활발히 진행되고 있는데 양자컴퓨팅 환경에서도 안전하게 사용할 수 있는 공개키 암호 기술인 양자내성암호와 더불어, 동형암호(암호화된 상태로 연산 가능한 암호), 형태보존암호(암호문이 평문과 동일한 형태를 가지는 암호), 경량암호(계산능력이 떨어지는 IoT 환경 등에서 효율적으로 사용할 수 있는 암호) 등이 있다.

<3> 암호의 공격, 분석, 평가

[1] 암호 공격

- 암호 공격 방식은 스트림 암호 알고리즘 공격 방식과 블록 암호 알고리즘 공격 방식으로 분류

(1) 스트림 암호 알고리즘 공격

- 구별 공격, 예측 공격, 키 복구 공격, 대수적 공격 등이 있음

1) 구별 공격

- 스트림 암호 알고리즘에서 생성되는 키 스트림과 난수열을 구별하는 공격
- 통계적인 분석 방법 및 대부분의 분석 방법이 이에 해당함

2) 예측 공격

- 이전의 적당한 길이의 키 스트림을 획득했다는 가정 하에 다음 발생할 수열을 예측하는 형태

3) 키 복구 공격

- 키 스트림을 이용하여 마스터 키 또는 내부 상태 값을 복구하는 공격
- 가장 강력한 공격 방식

4) 대수적 공격

- 알려진 입출력 쌍과 내부의 알고자 하는 값이 변수
- 암호 알고리즘의 과정을 통해 만들어진 과포화된 다변수 연립 방정식을 이용하여 변수의 값을 얻어 키를 복구하는 방법

(2) 블록 암호 알고리즘 공격

- 선형 공격, 차분 공격, 연관키 공격 등이 있음

1) 차분 공격

- 블록 암호의 비선형 함수에 대한 입력 차분과 출력 차분 값들의 확률 분포가 비균일함을 이용한 선택 평문 공격 방법

2) 선형 공격

- 여러 개의 선형 근사식을 이용해 비선형 근사식을 덧붙이는 방식

3) 연관키 공격

- 서로 다른 두 개의 키 사이의 연관관계를 알고 있으나 키 자체를 모를 때 각 키로부터 발생한 평문/암호문 쌍을 가지고 키를 알아내는 방법

[2] 암호 분석과 평가

- 암호 설계자는 알고리즘이 암호 분석가에게 알려질 것이라는 가정하에 설계해야 함

- 암호 분석(암호 해독)은 암호 시스템을 무력화시키려는 과학 또는 기술을 말함

(1) 암호 분석의 종류

1) COA

- 침해자가 특정 암호문만 가지고 이에 대응 되는 평문과 키를 찾으려는 것
- 침해자가 암호 알고리즘을 알고 있으며 암호문을 가로챌 수 있다고 가정함
- 평문의 통계적 성질과 문자의 특성들을 추정하여 해독
- 암호문만을 이용하기 때문에 주로 고전 암호 해독 방법으로 사용함

2) KPA

- 침해자가 특정 암호문과 별개로, 여러 개의 평문/암호문을 쌍으로 얻어, 약간의 평문에 대응하는 암호문을 알고 있는 상태에서 사용함
- 스니핑한 암호문에 대해서 암호화 방식을 추론하여 공격하거나, 암호문과 평문의 관계로부터 키나 평문을 추정하여 해독 또는 대칭키를 통해 이루어진 통신채널을 공격하는 것에 사용됨

3) CPA

- 침해자가 주어지는 평문/암호문 쌍을 선택할 수 있음
- 침해자가 송신자의 컴퓨터에 접속할 수 있다면 사용 가능
- 평문을 선택하고 그 평문에 해당하는 암호문을 얻어 키나 평문을 추정해 암호를 해독하는 방법으로 주로 공개키 시스템 공격 시 많이 사용 됨

4) CCA

- 침해자가 원하는 암호문을 선택하고 이에 대응 되는 평문을 얻어야 하기 때문에 침해자가 수신자의 컴퓨터에 접속할 수 있을 때 사용 가능함
- 복호화 방식을 알고, 키 값을 추정해 복호화하는 공격 방법으로 일부 암호문에 대한 평문을 얻어 암호를 해독함
- 주로 공개키 시스템 공격 시 사용함

(2) 암호 평가

- 암호 알고리즘을 평가할 때, 암호 시스템을 공격하기 위해 필요한 계산량이 매우 커서 현실적으로 공격할 수 없는 경우를 계산적으로 안전하다고 하며 무한한 계산 능력이 있어도 공격할 수 없는 경우에는 무조건적으로 안전하다고 함

- 암호 알고리즘을 만들 때는 암호 해독 비용이 암호화된 정보의 가치를 초과하거나 암호 해독 시간이 정보의 유효 기간을 초과하는 알고리즘을 개발해야 함

- 암호 기술 평가

1) 암호 알고리즘 평가

- 정보보호제품에 탑재된 암호 알고리즘에 대한 안정성 평가
- 알고리즘 자체만의 이론적 안정성만을 평가하며, 해당 알고리즘이 탑재된 제품이나 시스템과는

독립적으로 평가됨

2) 암호 모듈 평가

- 암호 알고리즘을 이용하여 제공되는 암호 서비스에 대한 안전성 평가
- 암호 알고리즘 자체의 이론적 안정성과 별개로, 암호 서비스 기능을 제공하는 암호 모듈의 안정성에 대한 평가

3) 정보보호제품 평가

- 암호 모듈을 탑재한 정보보호 제품에 대한 안정성을 평가하는 것

4) 응용시스템 평가

- 각 제품을 연동하여 구성되는 시스템에 대한 안정성 평가