Part 2. 암호학

Section 02. 암호학 개요 (출제빈도 2.1%)

1. 기본 개념

2. 암호기법의 분류

[치환 암호, 전치 암호]

[블록 암호, 스트림 암호]

- 블록 암호 : 평문을 특정 비트의 블록으로 잘라낸 후 암호화 알고리즘을 적용 EX) DES, AES
- 스트림 암호(Stream Cipher)
  - 평문을 한 문자씩 암호화하며 순차적으로 처리 (LFSR)
  - 내부 상태
  - 긴 주기와 높은 선형 복잡도
  - 블록 암호보다 빠르지만 암호화 강도가 약해 무선 데이터 보호에 적합

  [스트림 암호의 종류]

  - 동기식 스트림 암호(synchronous) EX) One-Time Pad, FSR, LFSR, NLFSR
    1. 암호화와 복호화에서 상호 동기화가 필수
    2. 전송도중 변조되어도 후속 암호문에 오류의 영향이 없다.
    3. 의도적인 변조를 복호화 단계에서 검출할 수 없음.
  - 자기 동기식 스트림 암호(self-synchronizing) = 비동기식 스트림 암호(asynchronous)
    1. 키 스트림 평문 or 암호문 스트림에 종속적
    2. 암호문이 전송도중 변경되어도 자기 동기화가 가능
    3. 변조된 암호문이 후속 암호문 복호화에 사용되지 않아 후속 암호문에 영향력이 없다.

3. 주요 암호기술에 대한 개괄

- 대칭키 암호
  1. 암호화 알고리즘은 평문에 transformation과 substitution을 적용하여 암호문을 만들어낸다. (O)
  2. 평문 속의 요소(비트, 문자를) 다른 요소 (비트, 문자 및 문자열)로 바꾸는 것을 transformation이라고 한다. (X) → substitiution

> 💡 바꾸는 것 → substitution
> 재배열 → transformation, transposition

4. 디지털 저작권 관리

- 스테가노그래피(steganography) : 메시지 자체를 은폐하는 기법
- 핑거프린팅(fingerprinting) : 구매자의 정보를 삽입

5. 암호 해독

[암호 분석의 종류]

- 암호문 단독 공격 (COA, Ciphertext Only Attack) : 암호문 C만을 갖고 평문 P나 키 K를 찾아내는 방법
- 기지 평문 공격(KPA, Known Plaintext Attack) : 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 방법
- 선택 평문 공격(CPA, Chosen Plaintext Attack)
- 선택 암호문 공격(CCA, Chosen CIphertext Attack)

6. 암호 알고리즘의 안정성 평가

- CMVP(Cryptographic Mdule Validation Program) : 암호모듈에 대한 안정성 평가

Section 03. 대칭키 암호 (출제빈도 3.3%)

- 관용 암호 = 공통키 암호 = 대칭키 암호 = 비밀키 암호

[1] 현대 대칭키 암호

1) 현대 블록 암호

- S박스, P박스
- 합성 암호(Feistel 암호, SPN 구조)
- 블록 암호에 대한 공격
  - 차분 분석, 선형 분석, 전수 공격법, 통계적 분석, 수학적 분석

2) 현대 스트림 암호

- 동기식 스트림 암호
  1. 키 스트림 평문 or 암호문은 스트림과 독립적
  2. 암호화, 복호화에서 상호 동기화 필수, 전송 도중 변조되어도 후속 암호문에 영향 X
  - One-Time Pad, FSR, LFSR, NLFSR
- 비동기식 스트림 암호
  1. 키 스트림 평문 or 암호문은 스트림에 종속적

2. 암호문이 전송 도중 변경되어도 자기 동기화 가능
3. 변조된 암호문이 후속 암호문 복호화에 사용되지 않아 후속 암호문에 영향 X

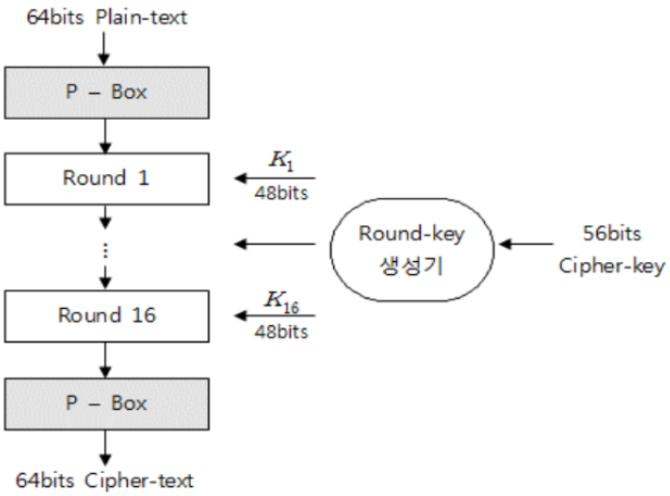
대칭 암호 알고리즘 : AES, DES, 3DES, ARIA, BlowFish,2 CRYPTON(한국)
비대칭 암호 알고리즘 : RSA, DSA, ECC, Diffie-Hellman, Rabin

Feistel : DES, Blowfish, MISTY, RC5, RC6, CAST256, SEED
SPN : SAFER, SHARK, Rijndael(=AES), Serpent (대부분 S로 시작), ARIA

- Feistel 구조의 특징
  1. 라운드 함수에 대한 제약 조건이 없음
  2. 2라운드의 수행으로 블록 간의 완전한 확산이 이루어짐
  3. 3라운드 이상이며 짝수 라운드로 구성
  4. 알고리즘 수행 속도가 빠르고, 하드웨어 및 소프트웨어 구현이 용이하며 아직 구조상 문제점이 없음
- SPN 구조의 특징
  - 복호화 시 라운드 함수의 역변환이 필요

[2] DES(Data Encryption Standard)

- IBM 제안, Feistel 구조, 64비트 키를 사용해 64비트의 평문을 전치, 대치 과정을 거쳐 암호화
  두 개의 P-Box, 16개의 Feistel 라운드 함수, 48bit의 라운드 키가 생성



[3] AES(Advanced Encryption Standard)

- NIST(미국 국립기술표준원)에서 공모한 암호 알고리즘, 라인달(Rijndal)이 채택
- non-Feistel 알고리즘, SPN 구조
- 키의 길이에 따라 라운드가 바뀜

[4] 대칭키 암호 알고리즘 (블록 크기/키의 길이/라운드 수)

1. DES (64/56/16)
2. IDEA (64/128/8)
3. Rijndael (128/128,192,256/10,12,14)
    - 2000년 AES 알고리즘으로 선정
4. RC5
    - 알고리즘 간단, 속도 빠름
5. SEED (128/128,256/16,24)
6. ARIA
7. HIGHT
8. LEA

대칭키 암호를 이용한 현대 암호화 기법

1. **ECB(Electronic CodeBook mode) : 전자 부호표 모드**
    - 평문블록을 암호화한 것이 그대로 암호문 블록이 된다.
    - 평문의 길이를 정확히 맞추기 위해 패딩(padding) 작업을 수행한다.
    - 가장 기밀성이 낮은 모드로, 암호문을 살펴보는 것만으로도 평문 속에 패턴 반복성을 감지
2. **CBC(Cipher Block Chaning) : 암호 블록 연쇄 모드**
    - 암호화되기 전에 이전 암호문 블록과 XOR된다.
    - 각각의 암호문 블록은 이전 평문 블록들의 영향도 받게 된다.
    - 초기화 벡터(initialization vector)가 존재하게 되는데, 첫 번째 평문 블록의 암호화를 위해 한개의 비트열 블록이 필요하다.
3. **CFB(Cipher-Feedback mode) : 암호 피드백 모드**
    - CBC와 다르게, '초기화 벡터'를 암호화한 후, 평문과 XOR하여 암호문을 생성
4. **OFB(Output-FeedBack mode) : 출력 피드백 모드**
    - 1단계에서 평문과 초기화벡터를 암호화한 블록을 XOR하여 암호문을 생성
    - 그 후, 초기화벡터를 암호화 한 것(output)을 암호 알고리즘으로 사용
    - 에러의 전이가 없고 키수열이 평문과 무관하여 미리 계산이 가능하고 또한 스트림 암호로 사용이 가능하다.
5. **CTR(Counter mode) : 카운터 모드**
    - 1씩 증가하는 카운터를 암호화해서 키 스트림을 만들어내는 스트림 암호다.

Section 04. 비대칭키 암호 (출제빈도 3.6%)

- 비대칭키 = 공개키

1. 비대칭키 암호

> 💡 소인수분해 문제 : RSA, Rabin
> 이산대수 문제 : ElGamal, DSA, ECC(타원곡선), Diffie-Hellman

[1] 대칭키 암호의 키 배송 문제

1. 키의 사전 공유
   - 키 관리 기관(Trusted Authority, TA)이 사전에 사용자들에게 비밀 경로를 통해 키를 전달
2. 키 배포 센터
   - 암호 통신이 필요할 때마다 키 배포 센터(KDC, Key Distribution Center)에서 키를 전달
3. DIffie-Hellman 키 교환에 의한 해결
   - 이산대수 문제(DLP)를 풀기 어렵다는 사실에 기반
   - 정보의 기밀성을 제공하지 못함 (중간자 공격)
4. 공개키 암호에 의한 해결

[2] RSA 암호 시스템

> 💡 DIfffie-Hellman : 키 교환
> RSA : 키 교환, 암호화/복호화, 디지털서명

- 교환하고자 하는 비밀키를 **수신자의 공개키**로 암호화하여 수신자 측에 전송하고, **수신자의 개인키**로 교환하고자 하는 비밀키를 복호화한다.

  [공격기법]

  - 수학적 공격, 전사적 공격, 시간 공격, 선택 암호문 공격

[3] Rabin 암호 시스템

[4] ElGamal

[6] 타원 곡선 암호(ECC, Elliptic CUrve Cryptosystem)

- RSA보다 짧은 길이의 키를 사용하면서 동일한 암호 강도를 지님
- 길이가 제한적인 무선 환경이나 작은 메모리를 가지고 있는 시스템에 적합

2. 하이브리드 암호 시스템

Section 05. 해시함수와 응용 (출제빈도 1.6%)

[1] 일방향 해시함수

- 일방향 해시함수 = 메시지 다이제스트 함수 = 암호학적 해시 함수

- 출력되는 해시값 = 메시지 다이제스트 = 핑거프린트

  [특징]

  - 임의 길이의 메시지로부터 **고정 길이**의 해시값을 계산
  - 충돌 내성(collision resistance) : 충돌을 발견하는 것이 어려운 성질

  [보안 요구사항]

  - 역상 저항성(=약 일방향성)
    - y=h(M)을 만족하는 입력 값 M을 찾는 것이 매우 힘들어야 함
  - 두 번째 역상 저항성 (=약한 충돌 내성 = 강 일방향성)
    - y=h(M)=h(M'), M≠M'을 만족하는 다른 입력 값 M'을 찾는 것이 매우 힘들어야 함
    - 어떤 M과 해시값 h=h(M)이 주어졌을 때, h(M')=h되는 서명문 M'을 찾는 것이 계산상 불가능해야 함
    - 어떤 주어진 블록 x에 대해서 H(x)=H(y)를 만족하는 y(≠x)를 찾는 것이 계산상 불가능해야 함
  - 충돌 저항성 (=강한 충돌 내성 = 충돌 회피성)
    - y=h(M)=h(M')을 만족하는 임의의 두 입력 값 M, M'을 찾는 것이 매우 힘들어야 함

[2] 암호학적 해시함수의 예

[키가 없는 해시 함수]

- MD2 → MD4 → MD5 (메시지 다이제스트)
  - MD5 : 메시지를 512bit 블록으로 나누고, 128bit 다이제스트로 출력 (너무 짧다는 문제)
- SHA (Secure Hash Algorithmn)
  - MD5보다 느리지만 안전
  - SHA

[키를 사용하는 해시 함수, MAC]

Section 06. ★ 전자서명과 KPI (출제빈도 4.0% / 매회 2문제~4문제 출제)

1. 전자서명

1. 전자문서의 서명은 다른 전자문서의 서명과 항상 동일해야 누구든지 검증할 수 있다. (X) → 재사용할 수 없음
2. 전자서명을 계산하기 위해 송신자는 문서에 대해 해시값을 계산한 후 그 값을 자신의 개인키로 암호화한다. (O)
3. 합법적인 전자서명만이 전자문서에 대한 전자서명을 생성할 수 있어야 한다. (O)
4. 서명 작성에 사용하는 키는 **송신자의 개인키**이고, 서명 검증에 사용하는 키는 **송신자의 공개키**이다.

5. 전자서명은 **송신자의 개인키**로 암호화하며 서명을 작성하고, 이는 **부인불가**조건을 만족시킨다. 또한 **송신자의 공개키**로 복호화하고, 이를 통해 전자서명 조건 중 **서명자 인증**을 만족시킨다.

> 💡 공개키 알고리즘
> **암호화 :** 수신자의 공개키
> **복호화** : 수신자의 개인키
>
> 전자서명
> **서명 작성** : 송신자의 개인키
> 서명 검증 : 송신자의 공개키

6. 전자서명 vs MAC(Message Authentication Code)

> 💡 전자서명 : 제3자에 대한 메시지를 검증하고 통신 상대의 부인방지를 행할 수 있는 인증 기술
> MAC : 무결성을 확인하고 메시지에 대한 인증을 하는 기술

[전자서명 서비스]

- 메시지 인증
- 메시지 무결성
- 부인방지

[전자서명 구조]

- RSA 전자서명
- ElGamal 전자서명
  - RSA 서명 길이의 2배이며, 거듭제곱의 계산량은 4배에 이름
- Schnorr 전자서명
- DSS (Digital Signature Standard)
  - ElGamal 전자서명을 개량 (이산대수 문제)
  - ElGamal 전자서명보다 계산량을 획기적으로 줄인 방식
- ECSDA (Elliptic Cruve DSA, 타원곡선 전자서명 구조)

[전자서명 방식]

- 복원형 전자서명
- 부가형 전자서명
- 특수 전자서명

[특수 전자서명]

- 공개키 방식 → 누구나 서명의 진위를 검증할 수 있음

1. 부인방지 전자서명
    - 서명자의 도움이 있어야 함
2. 의뢰 부인방지 서명
    - 신뢰하는 제 3자
3. 수신자 지정 서명
    - 지정한 검증자
4. **은닉 서명**
    - 서명문의 내용을 숨김
5. 위임 서명
    - 서명을 해야 할 사람이 부재중에 자신을 대리해서 서명을 할 수 있는 서명방식
    - 위임서명을 확인하는 검증자는 위임서명을 위임한 원래 서명자의 동의가 있었음을 확인하기 위해 서명자에게 확인 절차를 걸쳐야 한다. (X)
      → 확인절차를 거칠 필요가 없음.
6. 다중 서명

[전자 투표]

- PSEV : 터치스크린 기표기
- 키오스크 : 비지정 임의 투표소에서 전자투표, 관리자 없음
- REV : 가정, 직장에서 인터넷을 통해 투표

2. PKI (Public-Key Infrastructure, 공개키 기반 구조)

[개념]

- 제공 서비스 : 기밀성, 무결성, 인증, 부인방지, 접근제어

[PKI 구성요소]

- 인증기관(CA, Certificaiton Authority)
    - 인증 정책 수립 / 인증서 및 인증서 폐기목록 관리 / 다른 CA와의 상호 인증 제공
    - 인증서에 기반한 안전한 거래를 위해 세션키를 발급한다. (X)
    1. 정책 승인기관(PAA, Plicy Approving Authority)
        - 루트 인증 기관
        - 하위 기관 정책 감사
    2. 정책 인증기관(PCA, Policy Certification Authoriy)
        - 사용자들의 정책 수립
        - CA의 공개키를 인증하고 인증서, 인증서 폐지 목록 등을 관리
    3. 인증기관(CA, Certification Authority)

        - PCA 하위 계층
        - 사용자/등록기관의 요청에 공개키 인증서를 발행/폐지
- 검증기관(VA, Validation Authority)
    - 인증서 유효성 여부 / 관련 거래 유효성 여부 확인
- 등록기관(RA, Registration Authority)
    - 사용자와 CA가 원거리에 있는 경우, RA를 두어 사용자의 신분 및 소속 등을 확인
    - 인증기관(CA)을 대신해 사용자의 신분을 확인하고, 발급된 인증서 및 해당 CA 또는 상위기관의 **공개키**를 사용자에게 전달하는 역할
- 저장소(Repository, Directory)
    - 사용자의 인증서를 저장하는 일종의 DB
    - ITU-T에서 정의한 X.500 표준 형식과 이를 간략화시킨 LDAP(Lightweight DIrectory Access Protocol) 등이 있다.

LDAP(Lightweight DIrectory Access Protocol)
- 인증서 및 CRL 보관소에 저장되어 있는 PKI 정보 추가, 삭제, 변경을 수행하기 위한 프로토콜
- 보관소 읽기, 보관소 탐색 및 보관소 내용 변경 등의 역할

[PKI의 형태]

1. 계층 구조
    - 최상위 루트 CA 존재하며 트리형태로 CA가 분포
2. 네트워크 구조
    - 상위 인증기관의 영향 없이 독립적으로 존재 (복잡해짐)
3. 혼합형 구조

[PKI의 주요 관리 대상]

[인증서 표준 규격 X.509]

- 공개키 인증서(PKC, Public-Key Certificate)

[X.509 인증서 프로파일] = 인증서 표준 규격

- 버전 (필수)
- 일련번호 (필수)
- 서명 알고리즘 식별자 (필수)
- 발행자 이름 (필수)
- 유효기간 (필수)
- 주체이름 (필수)
- 주체의 공개키 정보 (필수)

- 발행자 유일 식별자 (선택)
- 주체 유일 식별자 (선택)
- 확장 (선택)
- 서명 (필수)

[X.509 V3 인증서 확장영역]

- 키 사용목적(Key Usage)
- 인증서 정책(Certificate Policies)
- 기관키 식별자(authority key identifier)
- 사용자키 식별자(subject key identifier)

[X.509 인증서 폐지 목록 프로파일]

- CRL(Certification Revocation List)

[인증서 운영 프로토콜]

온라인 인증서 상태 검증 프로토콜 (OCSP, Online Certificate Status Protocol)

- 실시간으로 인증서 상태 확인 가능한 프로토콜

Section 07. 키, 난수 (출제빈도 0.3%)

비대칭키 암호

Diffie-Hellman

- 최초의 공개키 알고리즘
- 이산대수의 계산의 어려움 (=ElGamal, 타원곡선, DSA 외우기 팁 EI산대수)
- 기밀성을 제공하지 못함

RSA

- 세션키를 이용
- 소인수 분해 문제의 어려움 (Rabin. 성능↓ OK)
- 전자서명 용도

RSA에 대한 공격

- 수학적 공격(소인수 분해 공격)
- 타이밍 공격(시간 공격)
- 선택 암호문 공격(CCA)와 OAEP

타원곡선암호(ECC, Elliptic Curve Cryptosystem)

- 스마트카드나 휴대폰 등 키의 길이가 제한적인 무선환경이나 작은 메모리 시스템에서 적합

해시함수

[해시함수의 보안 요구사항]

"y=h(x) → 해시함수(h)에 입력값(x)을 넣으면 해시값(y)가 생성됨

프리이미지 저항성 = 역상 저항성 = 일방향성 = 최초 해시값 y가 확인된 상태

> 입력값 x를 찾는 것은 계산상 불가능
> (1) 주어진 임의의 출력값 y에 대해, y=h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능하다.

제2프리이미지 저항성 = 두 번째 역상 저항성 = 약한 충돌 내성(=저항성) = 최초 입력값 x가 확인된 상태

> 동일한 해시값(y)이 나오는 다른 입력값(x')을 찾는 것은 계산상 불가능
>
> (1) 주어진 입력값에 대해 h(x)=h(x'), x(≠x')을 만족하는 다른 입력값 x'을 찾는 것이 계산적으로 불가능하다.
> (2) 메시지가 주어졌을 때 그 메시지가 동일한 해시 값을 갖는 다른 메시지를 발견해 내는 것이 매우 어렵다는 성질

충돌 저항성 = 충돌 회피성 = 강한 충돌 내성

> 동일한 해시 값(y)의 서로 다른 입력 값(x, x')을 찾는 것은 계산적으로 불가능
>
> (1) 동일한 다이제스트를 가지는 2개의 메시지를 구하지 못하도록 하는 것
> (2) h(x) = h(x')을 만족하는 임의의 두 입력값 x, x'을 찾는 것이 계산적으로 불가능하다.
> (3) 해시 값이 일치할 것 같은 서로 다른 두 개의 메시지를 발견해내는 것이 매우 어렵다는 성질
> (4) 충돌 저항성 h(x)=h(x')을 만족하는 임의의 두 입력값 x, x'을 찾는 것이 계산적으로 불가능하다.

[6] 전자서명과 KPI

전자서명

1. 전자서명의 개요
    1. 형식
    2. 과정
    3. 서비스
    4. 기능

1. 전자서명 구조(=기법)

1. RSA
    - 공개키
2. ELGamal
    - (191번)

    자신의 비밀키 x를Z_{p-1}에서 랜덤하게 선택하고, 공개키 $y = g^x \bmod p$를 계산하여 공개
3. Schnorr
    - (189번) 이산대수를 사용하는 전자 서명의 효율성을 높이기 위해 q|(p-1)인 소수 p, q의 사용을 처음 제안
4. 전자서명 표준(DSS, Digital Signature Standard)
    - **ElGamal 서명**을 개량한 방식해 계산량을 획기적으로 줄임
5. 타원곡선

전자서명 종류 기반 방식

전자서명	기반 방식	Column
RSA	소인수분해	
ElGamal	이산대수	
Schnorr	이산대수	
DSA	미국 NITS 제안	
SCDSA	DSA 타원곡선 버전	
KCDSA	국내 표준 전자서명	

1. 전자서명 방식
    1. 메시지 복원형
        - 서명자 : 서명자의 개인키를 이용해 메시지 암호화
        - 검증자 : 서명자의 공개키를 이용해 암호문 복호화
        - 장점 : 공개키 암호방식을 이용하므로, 별도의 **전자서명 프로토콜**이 필요하지 않음.
        - 단점 : 메시지를 일정한 크기의 블록으로 나누어 각각의 블록에 서명해야 하므로 **많은 시간이 소요**되어 실제로 사용하지 않음.
    2. 부가형
    3. 특수
2. 전자서명 응용
    1. 전자투표
        - PESV (Poll-site E-Voting) : 지정된 투표소에서 전자투표, 각 개표소는 폐쇄된 공공망으로 연결
        - 키오스크 방식 : 비지정 임의 투표소에서 전자투표. 투표소와 개표소를
        - REV (Remote Internet E-Voting) : 가정이나 직장에서 인터넷을 통하여 투표, 투표 결과가 개표소나 중앙관리센터로 보내짐
    2. 전자입찰

PKI(공개키 기반 구조, Public-Key Infrastructure)

1. PKI 개요
2. PKI 구성요소

1. 인증기관(CA, Certification Authority)
    - 폐지된 인증서 목록(CRL) 을 **생성**하는 역할을 함.
    1. 정책 승인기관(PAA, Policy Aprroving Authority)
    2. 정책 인증기관(PCA, Policy Certification Authority)
2. 검증기관(VA, Validiaton Authority)
    - 인증성의 유효성, 인증서의 적절 개체 발급되었다다는 것을 신뢰 당사자에게 확인시켜 줌.
3. 등록 기관(RA, Registration Authority)
    - 사용자와 CA가 원거리에 위치한 경우, 인증기관과 사용자 사이에 RA를 두어 신분과 소속을 **확인 및 등록**하는 기능 수행

    > 💡 (205번) 등록기관은 사용자 신분을 확인한 후 사용자 인증서를 발급한다.
    > → 정답 : X
    > → 해설 : '인증서 발행'은 인증기관(CA)의 역할이다.

4. 사용자와 최종 개체 (=사용자, 공개키 인증서 소유자)
5. 저장소(Repository, DIrectory)
    - LDAP (Leightweight Directory Access Protocol) : 조직이나 개체, 그리고 인터넷이나 기업 내의 인트라넷 등 네트워크상에 있는 파일이나 장치와 같은 자원 등의 위치를 찾을 수 있게 해주는 소프트웨어 프로토콜

3. PKI 형태

    [PKI] 보안에서 말하는 PKI 의 기본 개념 간단 설명
    https://crazia.tistory.com/entry/PKI-PKI-%EC%9D%98-%EA%B8%B0%EB%B3%B8-%EA%B0%9C%EB%85%90-%EA%B0%84%EB%8B%A8-%EC%84%A4%EB%AA%85

    1. 계층 구조
    2. 네트워크 구조
    3. 혼합형 구조
4. PKI 주요 관리 대상
    1. 인증서(PKC, Public-Key Certificate)
        1. 인증서 표준 규격 X.509
        2. 인증서 확장 영역
            - X.509 V3 인증서 확장영역은 **사용자의 공개키 정보**와 **연관된 추가 정보 제공**
                - 기관키 식별자
                - 사용자키 식별자
                - 키 사용
                - 인증서 정책

2. X.509 인증서 폐지 목록 프로파일
    1. CRL (Certificate Revocation List)
        - 기본 확장자 : CA 키 고유 번호, 발급자 대체 이름, CRL 발급 번호, 발급 분배점, 델타 CRL 지시자
        - 개체 확장자 : 취소 이유 부호, 명령 부호, 무효화 날짜
    2. 인증서 운영 프로토콜

외우기 TIP

1. DSS : 이산대수(DS), ElGamal : 이(EI)산대수