**정보보안기사**

**2장 암호학**

**1절 암호학개요(최종수정일 7/22)**

**암호학의 관례적 표현**

**앨리스** – 송신자

**밥** – 수신자

**이브** – 도청자(기밀성 침해, 정보 수정은 x)

**맬로리** – 메시지 수정, 재전송

**트렌트** – 신뢰할 수 있는 중재자(중립적인 제 3자)

**빅터** – verifier 의도된 거래나 통신 검증

**암호화와 복호화의 기호적 표현**

**평문** – M or P

**암호문** – C

**암호 알고리즘** – E

**복호 알고리즘** – D

**키** – K

* == : 평문 P를 k로 암호화해 암호문 C를 얻는다.
* == : 암호문 C를 k로 복호화해 평문 P를 얻는다.

**암호 알고리즘과 키의 분리**

암호화 시 알고리즘은 재사용하지만 키는 재사용하지 않는다. 둘을 분리해서 생각해야 한다.

**암호와 보안 상식**

* **비밀 암호 알고리즘을 사용하지 말 것:** 암호 알고리즘 자체를 비밀로 해 기밀성을 유지하는 암호 시스템은 알고리즘 구조가 드러나는 순간 파훼된다. 이는 숨기는 것에 의한 보안(Security by obscurity)이다. 일반적으로 비전문적이고 어리석은 행위로 여겨진다.
* **약한 암호는 암호화하지 않는 것보다 위험하다:** 단순히 ‘암호’라는 수단에 의지해 허술한 체계에 보안을 맡길 경우 기밀성이 높은 정보를 소홀히 취급할 위험이 있다. 허술한 암호를 사용할 바에는 암호 자체를 사용하지 않고 중요하게 취급하는 편이 낫다.
* **어떤 암호라도 언젠가는 해독된다:** 모든 키를 하나도 빠짐없이 시도해보면 언젠가는 복호화된다. 암호화는 쉽고 빠르지만 복호화가 어려운 시스템을 만들기 위해 트레이드오프를 신경써야 한다.
* **암호는 보안의 작은 부분일 뿐이다:** 최근에는 피싱, 트로이목마, 키로거 등 보안의 약한 고리인 사람을 향한 사회공학적 공격이 자주 행해진다. 시스템의 보안 강도는 가장 약한 링크의 강도와 같다. 모든 링크가 골고루 강한 시스템이 보안성이 강한 시스템이다.

**암호기법의 분류**

**치환암호와 전치암호, 블록암호와 스트림 암호, 위치에 따른 암호화 구분, 하드웨어와 소프트웨어 암호 시스템 등으로 구분된다.**

**치환암호와 전치암호**

**치환암호(대치 암호, Substitution Cipher):** 비트, 문자, 문자열을 다른 비트, 문자, 문자열로 대체한다. 교환 규칙은 일대일 대응이 아니어도 상관없다.

**전치암호(Transposition Cipher):** 원문을 재배열해 의미를 숨긴다. 평문의 문자와 암호문의 문자가 일대일로 대응한다.

**+ 키 공간의 크기와 비트수**

키 공간이 클수록 공격으로부터 안전하다. 하지만 키 공간에 할당할 비트수가 증가하게 된다.

예를 들어 키 공간의 크기가 8!이면 8비트 숫자에 대한 전치 암호화를 위한 키의 비트수는 []이 되고 8비트로 구성되는 숫자를 8비트의 다른 숫자로 치환하는 암호화의 경우 키 공간의 크기가 이므로 키의 비트수는 []가 된다. (키 공간의 크기: 암호화 키가 가질 수 있는 경우의 수의 총합, 키 비트수: [])

**블록 암호와 스트림 암호**

**블록암호(Block cipher):** 특정 비트 수의 집합을 한 번에 처리하는 암호 알고리즘. 집합 -> 블록, 블록의 비트 수 -> 블록 길이, 블록의 크기는 보통 ASCII(8비트) or Unicode(16비트)에 비례, 스트림 암호와 달리 Round를 사용, 반복적으로 암호화해 암호화 강도를 높인다.

**스트림암호(Stream cipher):** 한 번에 1비트 or 1바이트씩 스트림을 순차적으로 암호화, 평문과 키 스트림을 XOR해 암호를 생성한다. 블록 암호는 블록 단위로 처리해 내부 상태를 가지지 않지만 스트림 암호는 순차적으로 처리하기에 내부 상태를 가진다. 군사/외교용으로 널리 사용, 일부 상용, 이동 통신 환경에서 구현이 용이, 안정성을 수학적으로 엄밀하게 분석할 수 있어 이동 통신 등의 무선 데이터 보호에 적합

|  |  |  |
| --- | --- | --- |
| 구분 | 블록 암호 | 스트림 암호 |
| 장점 | 암호화 속도 빠름, 에러 전파 없음 | 높은 확산, 기밀성, 해시함수 등 다양 |
| 단점 | 낮은 확산 | 느린 암호화, 에러 전달 |
| 사례 | LFSR(Linear Feedback Shift Register), MUX generator | DES, IDEA, SEED, RC5, AES |
| 암호화 단위 | 비트 | 블록 |
| 주요 대상 | 음성, 오디오/비디오 스트리밍 | 일반 데이터 전송, 스토리지 저장 |

**위치에 따른 암호화의 구분(링크, 종단간 암호화)**

**링크 암호화(Link Encryption):** 패킷은 홉에서 해독된다. 라우터는 패킷의 헤더를 해독하고, 해더 내의 라우팅과 주소 정보를 읽고 그것을 다시 암호화해 진행 방향으로 보낸다. 링크 암호화는 데이터 링크 또는 물리 계층에서 일어난다. 하드웨어 암호화 장치들은 물리계층의 인터페이스를 가지고 그것을 통과하는 모든 데이터를 암호화한다.

**종단간 암호화(End-to-End Encryption):** 헤더와 트레일러가 암호화되지 않기 때문에 패킷을 각 홉에서 해독하고 암호화하지 않는다. 애플리케이션 계층에서 송신자와 수신자 사이에 일어나는 암호화이기 때문에 사용자가 암호화할 메시지를 선택할 수 있는 유연성을 제공한다.

|  |  |  |
| --- | --- | --- |
| 구분 | 링크 암호화 | 종단간 암호화 |
| 특징 | ISP나 통신업자가 암호화,  헤더를 포함한 모든 데이터를 암호화,  유저가 알고리즘 통제 불가 | 사용자가 암호화,  헤더(라우팅정보)는 암호화 x,  알고리즘에 대한 통제는 사용자가 한다. |
| 장점 | User-transparent하게 암호화되어 운영이 간단,  트래픽분석을 어렵게 함,  온라인으로 암호화 | 사용자 인증 등 높은 수준의 보안 서비스를 제공,  중간노드에서 데이터가 암호문으로 존재 |
| 단점 | 중간 노드에서 데이터가 평문으로 노출,  다양한 보안서비스를 제공하는 한계,  모든 노드가 암호화 장비를 갖춰야 해서 네트워크가 커지면 비용이 커진다. | 트래픽 분석에 취약,  오프라인으로 암호화 |

**하드웨어와 소프트웨어 암호시스템**

**하드웨어 암호시스템:** 컴퓨터의 내부 버스와 외부 인터페이스에 전용 암호처리 하드웨어를 설치해 데이터를 암호화, 전용 하드웨어로 암호화해 CPU에 부담을 주지 않고 빠르게 암호화 가능

**소프트웨어 암호시스템:** 저렴한 비용과 적당한 안정성, 처리속도. CPU 성능 향상으로 주류 암호시스템이 되었다.

**주요 암호기술 개괄**

1. **대칭키/비대칭키 암호:** 암호화/복호화 키가 동일하면 대칭키, 다르면 비대칭키 암호. 대칭키는 공개키에 비해 빠르고 암호키의 길이가 공개키 방식보다 작아서 일반적인 정보의 기밀성을 유지하기 위한 용도로 사용된다. 반면 비대칭키 암호는 공개키 암호라고도 하며 대칭키 방식보다 속도가 느려서 키 분배나 전자서명, 카드번호와 같은 작은 크기의 데이터를 암호화할 때 많이 사용한다.
2. **하이브리드 암호:** 대칭키/공개키 방식의 장점을 조합한 암호 시스템
3. **일방향 해시함수:** 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해시값 또는 해시 코드라 불리는 값을 생성, 동일한 입력에는 항상 동일한 값 생성, 해시값만으로는 입력 메시지를 유추할 수 없어 비밀번호와 같이 복호화 없이 입력값의 정확성 검증이 필요한 경우 사용.
4. **메시지 인증코드:** 메시지의 송신자 확인코드(message authentication code), 메시지가 생각했던 송신자로부터 왔는지, 중간에 변경되지는 않았는지 확인하는데 쓰인다. 무결성과 인증 제공
5. **전자서명:** 오프라인의 서명/날인, 도장 개념을 온라인에 적용한 것. 거짓행세(spoofing), 변경, 부인이라는 위협을 방지하는 기술. 무결성 확인, 인증과 부인방지를 위해 사용
6. **의사난수 생성기:** PRNG, Pseudo Random Number Generator. 난수열 생성 알고리즘. 난수는 key generator라는 중요한 역할을 담당한다.

**암호 분석(해독)**

암호해독(cryptanalysis)이란 정규 참여자가 아닌 제3자가 암호문으로부터 평문을 찾으려는 시도이다. 공격이라고도 하며 암호 해독에 참가하는 사람을 제3자 또는 침해자라고 한다.

평문의 통계적 성질과 암호에 관한 지식, 장비, 그 밖의 정보를 통해 평문 혹은 키를 찾아낸다. 암호 해독자는 현재 사용되고 있는 암호 방식을 알고 있다는 전제 하에서 암호 해독을 시도하는 것으로 간주한다. 이를 **케르히호프의 원리**라고 한다.

* **케르히호프(kerckhoff)의 원리:** 암호시스템의 안전성은 암호 알고리즘의 비밀을 지키는데 의존해서는 안 되고 키의 비밀을 지키는데 의존해야 한다는 원리

**암호 분석의 분류**

**암호문 단독 공격(COA, Ciphertext Only Attack):** 이브가 암호 알고리즘을 알고있고 암호문을 가로챌 수 있다. 이브가 오직 암호문만을 통해 키와 평문을 찾아내야 하는 상황이다.

**기지 평문 공격(알려진 평문 공격, KPA, Known Plaintext Attack):** 이브가 해독하려는 암호문 외에 여러 개의 평문/암호문 쌍을 알고있다. 이브는 공개된 평문/암호문의 관계로 앨리스가 밥에게 보낼 정보를 파악한다.

**선택 평문 공격(CPA, Chosen Plaintext Attack):** 이브가 공격자에게 주어지는 평문/암호문 쌍을 선택할 수 있는 공격이다. 이브가 앨리스의 컴퓨터에 접속할 수 있다면 가능하다. COA나 KPA와 달리 CPA는 공격자가 암호화 과정에 영향을 미친다는 점에서 능동적이므로 능동적 공격자라고 할 수 있다.

**선택 암호문 공격(CCA, Chosen Ciphertext Attack):** 이브가 암호문을 선택하고 그에 대응하는 평문을 얻는다는 점을 제외하면 CPA와 유사하다. 이브가 밥의 컴퓨터에 접속할 수 있다면 가능하다. 선택된 암호문을 복호화할 수 있는 기계를 “Decryption Oracle, 복호 오라클”이라고 한다. 선택 암호문 공격에 견딜 수 있는 암호 알고리즘은 강한 알고리즘이다.

**+ 고무호스 암호분석(Rubber-Hose Cryptanalysis):** 암호분석가가 키를 얻을 때까지 키를 가진 사람을 공갈, 협박, 고문하여 키를 획득하는 방법. 가장 강력한 공격이다.

**암호 알고리즘의 안정성 평가**

**안전성 개념:** 안전성에는 두 가지 관점이 있다.

1. **계산적으로 안전 -> 암호시스템을 공격하기 위해 필요한 계산량이 매우 커 현실적으로 공격할 수 없는 경우**
2. **무조건적으로 안전 -> 무한한 계산능력이 있어도 공격할 수 없는 경우(ex. 암호 해독 비용이 암호화된 정보의 가치를 초과, 암호 해독 기간이 정보의 유효 기간을 초과)**

**암호제품 평가체계:** CC(Common Criteria) -> 1998 미,캐,영,프,독 간에 체결(1부. 시스템 평가 원칙/모델, 2부. 시스템 보안 기능 요구사항(11개), 3부. 시스템 7등급 평가를 위한 보증 요구사항(8개), CC의 평가기준에는 알고리즘에 대한 평가기준이 없어 각국에 독자적으로 맡긴다는 한계가 있다. -> 미국의 NIST가 수행하는 CMVP(Cryptographic Module Validation Program)이 암호모듈(암호 알고리즘을 통한 암호 서비스)에 대한 안정성 평가를 대신한다. **CC와 CMVP**

**암호기술 평가**

1. **암호 알고리즘 평가:** 알고리즘만 평가해서 탑제된 제품/시스템과 독립적으로 평가가 가능, 알고리즘 자체의 이론적 안전성만 평가
2. **암호모듈 평가:** 암호 알고리즘을 통한 암호 서비스(기밀성 기능 모듈, 무결성 기능 모듈)에 대한 안전성 평가. -> **CMVP**
3. **정보보호제품 평가:** 암호모듈을 탑재한 정보보호제품(침입차단시스템, 침입탐지시스템 등등) 안전성 평가
4. **응용시스템 평가:** 각 제품을 상호 연동해 구성한 시스템(국가기관망, 항공관제센터)에 대한 안전성 평가

**암호 알고리즘 암호모듈 정보보호제품 응용 시스템**

**평가과정:** 일반적으로 위 집합 관계의 순서를 따른다.

**암호모듈의 안전성 평가(CMVP):** 미국 NIST와 캐나다 CES(Communications Security Establishment)가 공동개발. 분류 -> 1. 암호 기술의 구현 적합성 평가 2. 암호키 운용 및 관리 3. 물리적 보안, 국내 암호모듈 검증 체계는 검증기관과 시험기관으로 구분한다. 국정원은 검증기관, 국가보안기술연구소와 한국인터넷진흥원은 시험기관

**지적 재산권 보호**

**디지털 저작권 관리**

1. **스테가노그라피(Steganography):** 암호화는 메시지를 통해 비밀을 기록하는 것인 반면 스테가노그라피는 메시지 자체를 다른 무언가(이미지, mp3)로 감추어버리는 것이다.
2. **디지털 워터마킹(Digital Watermarking):** 콘텐츠를 왜곡하지 않는 범위 내에서 저작권 정보를 디지털 콘텐츠에 삽입하는 기술. 강한 워터마킹과 공격을 받으면 쉽게 파괴되는 약한 워터마킹으로 구분된다.
3. **핑거프린팅(Fingerprinting):** 콘텐츠에 구매자의 정보를 넣어 불법배포 시 구매자 추적
4. **디지털 저작권 관리(DRM, Digital Rights Management):** 콘텐츠 소유자가 콘텐츠에 대한 접근 권한을 다양한 방식으로 제어할 수 있는 기술적 방법 집합(오디오, 비디오, 이미지, 텍스트, 멀티 미디어, 소프트웨어의 실행 보기 복제 출력 변경…)

**+ DRM 구성요소**

1. **메타데이터:** 콘텐츠 생명주기 안에서 관리해야 할 각종 데이터의 구조 및 정보
2. **패키저:** 보호 콘텐츠를 메타데이터와 함께 Secure Container 포맷으로 패키징하는 모듈
3. **시큐어 컨테이너:** DRM의 보호 범위 내에서 유통되는 콘텐츠의 배포단위
4. **식별자:** 콘텐츠를 식별하기 위한 식별자
5. **DRM 제어기(DRM Controller):** 콘텐츠를 이용하는 사용자의 PC또는 디바이스에서 콘텐츠가 라이선스에 명시된 범위 내에서 지속적으로 보호받을 수 있도록 프로세스를 제어한다.

**+ DRM 모델**

DRM 사용자 그룹은 크게 제공자, 배포자, 소비자, 클리어링하우스로 나눈다.

**제공자:** 콘텐츠에 대한 디지털 권리를 가지로 권리 보호를 원하는 DRM 사용자. 권리표현언어 -> REL(Rights Expression Language), 대표적 REL == ODRL(Open Digital Rights Language) && MPEG(Moving Picture Expert Group) REL

**배포자:** 온라인 쇼핑몰 같은 콘텐츠 유통 채널을 제공하는 DRM 사용자 소비자에게 콘텐츠를 제공하고 클리어링하우스로부터 대금을 분배받는다.

**소비자:** 클리어링하우스를 통해 콘텐츠 권리를 요청하고 합당한 대금을 지불한다.

**클리어링하우스:** 소비자에게 디지털 허가를 발급하고 제공자에게 로열티 수수료를 지불하며 배포자에게 배급 수수료를 지불하는 거래를 취급한다. 또한 모든 소비자의 사용내역을 기록하는 책임을 진다.

**3절 대칭키 암호**

**현대 대칭키 암호**