6차시. 4차 산업혁명사이버 보안의 핵심 '암호'

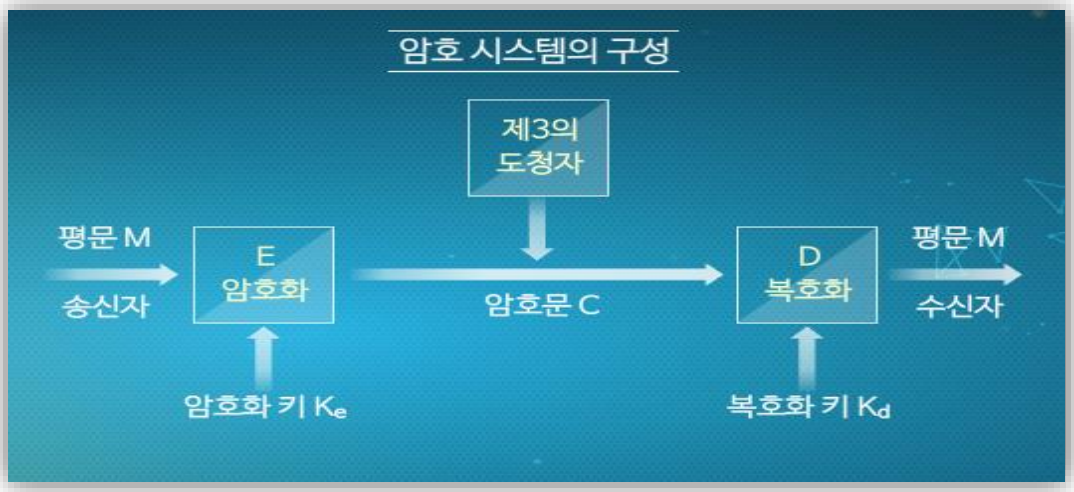
01. 암호의 역사와 종류

- 최근 4차 산업혁명 시대의 예고와 함께 사회 전 분야에 걸쳐 정보보호 관련 사고 발생 및 피해사례가 속출하는 가운데 정보보호에 대한 인식이 증가하면서 암호기술 이용에 대한 필요성이 더욱 강조되고 있다. 암호기술은 현재 인터넷뱅킹, 사이버증권, 신용카드결제, 전자입찰, 전자화폐, 저작권이나 산업정보, 개인정보 보호, 전자선거 등 다양한 분야에서 정보의 기밀성 및 무결성, 사용자 인증 등을 위해 절대적으로 필요한 기술이다.
- 그러나 이러한 필요성 증대에도 불구하고 국내 암호 솔루션 도입 현황은 저조한 실정이다. 실제로 한국인터넷진흥원에서 조사한 국내 IT서비스 제공업체의 암호 솔루션 사용현황에 따르면, 금융기관을 제외한 교육, 의료, 전자거래 업체 등의 암호 솔루션 사용현황이 40%이하로 낮게 나타났다. 또한, 동일한 조사에서 암호 솔루션 도입 필요성에 대한 CEO의 인식부족 및 비용 부담, 관련 전문가 및 분야별 암호적용 범위 수준 등에 구현 가이드라인 부재 등이 암호 솔루션의 도입을 미루는 이유로 나타났다. 따라서 이번 차시에서는 암호에 대한 기본 개념에서부터 암호기술 전반에 대한 개념을 파악하는 목적으로 다소 기술적인 내용에 초점을 맞추어 학습을 한다.

암호의 개념

- 암호(cryptography)의 어원은 그리스어의 말로 비밀이란 뜻을 가진 크립토스(Cryptos)에서 유래된 것으로 알려져 있다. 즉, 암호는 평문을 해독 불가능한 형태로 변환하여 암호문으로 생성하고 암호문을 원래의 해독 가능한 상태인 평문으로 변환하는 적용되는 모든 수학적인 원리, 수단, 방법 등을 취급하는 기술 또는 과학을 말한다. 간략히 말하면, 중요한 정보를 다른 사람들이 보지 못하도록 하는 방법이다.
- 그러나 현대의 정보화 사회에서는
  - 정보를 감추는 기밀성뿐만 아니라
  - 정보에 대한 적법한 권한을 가지고 있는지를 확인하는 인증 및 접근통제,
  - 정보의 변조 여부를 확인하는 무결성,
  - 정보에 대한 사용자의 서명 등 좀 더 다양한 기능들을 요구한다. 현대의 암호는 이런 기능들을 구현하기 위한 모든 수학적 기반기술이라고 말할 수 있다.
- 암호는 고도의 수학적인 내용을 포함하고 있어서 일반인들이 접근하기 어려운 순수 학문처럼 보이지만, 실제로는 정보보호 적용을 목표로 하는 매우 실용적인 학문이라고 말할 수 있다. 안전한 암호를 사용하는 것만으로 모든 정보를 보호할 수 있다고 생각할 수는 없겠지만, 암호를 사용하지 않고 궁극적인 정보보호를 성취하는 것은 불가능하다.

- 따라서 4차 산업혁명의 시대에서 인공지능, 사물인터넷, 커넥티드카, 모바일 등에서 필수적으로 사용되고 있으며 눈에는 보이지 않지만 우리의 안전을 지켜주는 역할을 하며 그 중요성이 강조되고 있다.
- 다음 그림은 암호 시스템이 어떻게 구성되는지 보여준다. 송신자와 수신자는 비밀리에 메시지를 주고받고자 한다. 송신자와 수신자는 자신들이 직접 소유하고 관리하는 컴퓨터를 이용하며, 인터넷과 같은 공개된 공용 통신망을 통해 통신을 한다. 송신자는 보내고자 하는 평문을 암호화 알고리즘을 이용해 암호문으로 변환하고, 이것을 공용 통신망을 통해 수신자에게 보낸다. 수신자는 복호화 알고리즘을 이용해 평문을 복구한다. 이때 암호화키는 송신자에 의해 암호화 알고리즘에 사용되고, 복호화키는 수신자에 의해 복호화 알고리즘에 사용된다.



- 도청자(eavesdropper)는 정당한 참여자가 아닌 제삼자로서 통신망에서 관찰되는 암호문으로부터 암호해독(cryptanalysis) 기술을 이용해 평문을 해독하고 통신되는 메시지에 대한 정보를 획득하고자 하는 사람을 말한다. 제삼자는 메시지의 도청과 같은 수동적인 공격뿐만 아니라 메시지를 위조하거나 전달을 방해하는 등 좀더 능동적인 공격을 가할 수 있는데, 이들을 통칭하여 공격자(attacker)라고 한다.

잠깐! 용어 학습하기

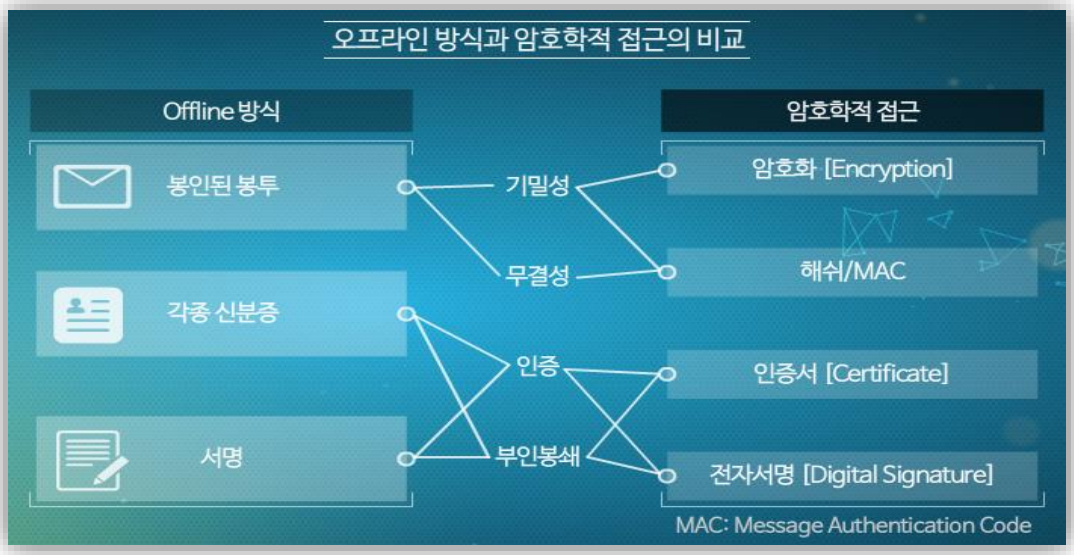
- 평문(Plaintext) : 원래 메시지(original message)
- 암호문(Ciphertext) : 암호화된 메시지(coded message)
- 암호(Cipher) : 평문을 암호문으로 변환하는데 적용된 알고리즘
- 키(Key) : 송신자/수신자에게만 알려진 암호에서 사용된 정보
- 암호화기(Encipher (encrypt)) : 평문을 암호문으로 변환
- 복호화기(Decipher (decrypt)) : 암호화문에서 평문을 복원
- 암호기법(Cryptography) : 암호 원리와 방법을 연구

잠깐! 용어 학습하기

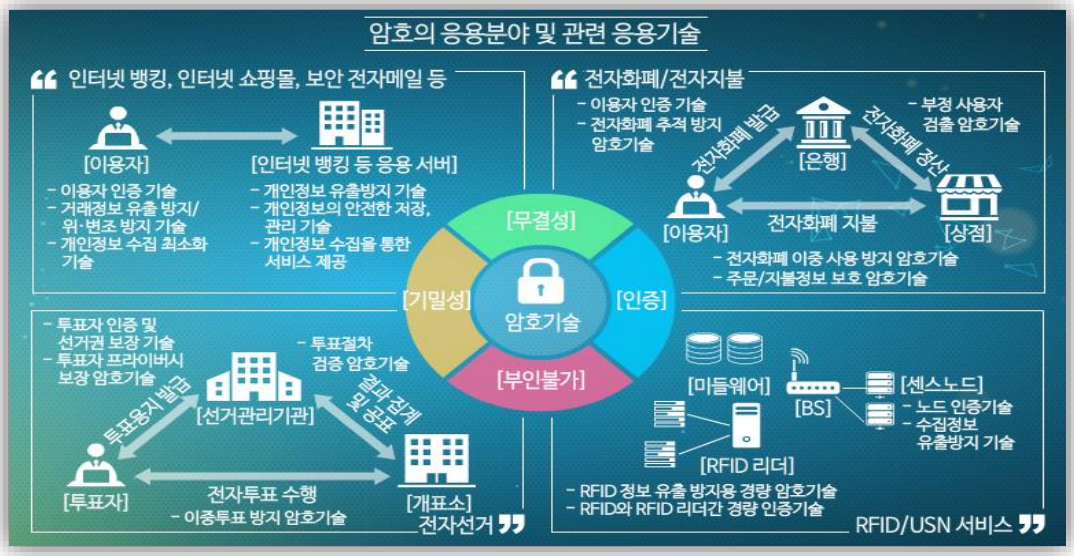
- 암호분석(Cryptanalysis) : 알려진 키 없이 암호문을 복호화하는 원리와 방법을 연구
- 암호학(Cryptology) : 암호기법과 암호분석 두 가지 영역을 포함

- 이러한 암호를 사용하는 목적은 크게 아래의 4가지로 정리된다
  - 기밀성 유지 (Confidentiality): 누가 엿듣지는 않나?
    . 인가자만 정보 접근 허용
  - 무결성 유지 (Data Integrity): 누가 내용을 바꾸지는 않나?
    . 위조/변조 여부를 확인
  - 출처 인증 (Authentication for Entity and Data): 상대방이 맞나?
    . 정보의 생산이 정당한지 검증하는 과정으로 정당한 사용자인지 또는 정당한 출처에서 생성된 자료인지를 보장
  - 부인방지 (Non-repudiation): 누구 말이 옳은가?
    . 행위에 대한 부인 방지

- 다음 그림에서와 같이 종래의 오프라인 방식에서는 봉인된 봉투, 각종 신분증, 인감을 비롯한 서명 등을 조합하여 기밀성, 무결성, 인증 및 부인봉쇄 기능을 수행하였다.



- 다음 그림은 암호의 응용분야와 함께 관련 암호응용기술을 함께 도시하였다. 인터넷 뱅킹이나 인터넷 쇼핑몰 분야에서는 개인정보유출 방지나 이용자 인증기술이 중요한 역할을 하며 전자선거에서는 이중투표 방지 암호기술 등이 핵심기술이 된다.



암호의 개념

암호 시스템 둘러보기-역사

암호 기술의 발전 역사를 구분할 때 흔히 고대 암호, 근대 암호, 현대 암호 등의 세 단계로 나눠진다. 첫 번째 전환점은 1920년대, 1, 2차 세계 대전에서 무선 통신 기술의 발전을 기반으로 여러 가지 기계적, 전자적 암호 장치를 개발하고 사용한 것이었고, 두 번째 전환점은 1970년대 들어 컴퓨터 사용이 활발해지면서 컴퓨터를 이용한 암호 기술이 발전한 것이다. 이러한 전환점을 기준으로 고대로부터 1, 2차 세계 대전 이전가지 사용된 초보적인 암호 기술들을 고대 암호라고 하면, 1970년대까지 복잡한 기계 장치와 전자 장치들을 이용한 암호 기술을 근대 암호, 컴퓨터가 개발된 이후 컴퓨터를 이용하는 암호 기술을 현대 암호라고 부른다.

고대 암호(1세대: 고대~19세기말)

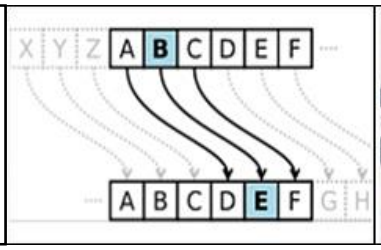
고대 봉건 사회에서는 황제나 군주가 지방 관리에게 보내는 비밀문서, 전쟁 중의 작전 지시와 보고, 첩자들과의 통신 등 전쟁이나 첩보 시에 정보를 전달해야 하는 경우에 다양한 비밀 통신 기법들이 사용되었다. 예를 들어, 종이에 쓴 메시지가 그냥 보이지 않지만 불빛에 약품 처리를 하면 메시지가 나타나도록 하는 방법, 비밀 노출을 방지하기 위해 말로 전달하도록 하는 방법 등이 다양하게 사용되었다. 이러한 비밀 통신 방법을 스테가노그래피(Steganography)라고 하는데 적들도 이 통신 방식을 알고 있으면 비밀을 유지하기 어렵다는 한계를 갖고 있다.

기원전 400년경 고대 그리스의 군사들은 스키테일 암호라고 불리는 전치 암호(문자의 위치를 서로 바꾸는 암호, transposition cipher)를 사용한 기록이 있다. 특정 지름을 갖는 막대에 종이를 감고 평문을 횡으로 쓴 다음 종이를 풀면 평문의 각 문자는 재배치되어 정보를 인식할 수 없게 되는데, 암호문 수신자가 송신자가 사용한 막대와 지름이 같은 막대에 종이를 감고 횡으로 읽으면 평문을 읽을 수 있다. 여기서 막대의 지름은 송신자와 수신자 사이에 공유된 비밀키가 된다.

로마의 황제였던 줄리어스 시저(Julius Caesar)는 시저 암호라고 불리는 환자 암호(문자를 다른 문자로 치환하는 암호, substitution cipher)를 사용하였다. 시저는 가족과 비밀 통신을 할 때 각 알파벳순으로 세자씩 뒤로 물려 읽는 방법으로 글을 작성했다. 즉 A는 D로, B는 E로 바꿔 읽는 방식이었다. 수신자가 암호문을 복호화하려면 암호문 문자를 좌측으로 3문자씩 당겨서 읽으면 원래의 평문을 얻을 수 있다. 송신자와 수신자는 몇 문자씩 이동할지를 비밀키로 하여 바꿔가면서 사용할 수 있다. 시저는 브루투스에게 암살당하기 전 가족들로부터 'EH FDUHIXO IRU DVVDVVLQDWRU'라는 긴급 통신문을 받았다. 3글자씩 당겨서 읽어보면 'BE CAREFUL FOR ASSASSINATOR'라는 '암살자를 주의하라'는 것이었다. 결국 암호문을 전달받은 당일 시저는 원로원에서 전혀 생각지도 못했던 브루투스에게 암살당하면서 "브루투스, 너마저……."라는 말을 남겼다.

악보 암호는 전설적인 스파이 마타하리(본명은 마그레타 G. 젤러, Margaretha Geertruida Zelle)가 사용했던 방식이다. 마타하리는 일명 '첩보원 H21'이란 이름으로 프랑스 장교에 접근해 군사 기밀 정보를 독일에 빼돌렸는데, 이때 비밀 통신에 사용된 암호가 악보였다. 일정한 형태의 음표에 알파벳 하나씩을 대응시킨 형태로 얼핏 보기에 평범한 악보처럼 보이지만, 실제로 연주하면 전혀 '음악'이 되지 않는다. 마타하리의 첩보 활동은 20여만 명에 달는 프랑스군을 죽음으로 몰고 갔다. 그녀는 제 1차 세계 대전이 끝나기 1년 전 프랑스 정보부에 체포돼 사형 당했다.

[스키테일 암호]



[시저 암호]

[악보암호]

2세대 암호

20세기 들어서는 통신 기술의 발전과 기계식 계산기에 대한 연구를 바탕으로 두 차례의 세계 대전을 통해 암호 설계와 해독에 대한 필요성이 높아지면서 암호에 대한 연구가 더욱 활발하게 진행되었다. 근대 암호의 이론적 기초가 된 논문은 1920년 Freidman이 발표한 '일치 반복률과 암호 응용'과 1949년 Shannon이 발표한 '비밀 시스템의 통신 이론'을 들 수 있다. Shannon은 논문에서 일회성 암호 체계가 안전함을 증명했고, 암호 체계 설계의 두 가지 기본 원칙인 '혼돈과 확신 이론'을 제시하였다. 암호 체계를 설계함에 있어 '혼돈(Confusion)'은 평문과 암호문 사이의 상관관계를 숨기는 반면, '확산(Diffusion)'은 평문의 통계적 성격을 암호문 전반에 확산시켜 숨기는 역할을 한다. 혼돈과 확산이라는 두 가지 개념은 오늘날의 암호 체계 설계에도 여전히 적용되고 있다.

Freidman은 2차 세계 대전 중 독일군이 사용하던 에니그마(Enigma) 암호와 일본군이 사용하던 무라사끼 암호를 해독한 사람으로 유명하다. 에니그마 암호는 각기 다른 몇 개의 암호판을 전기적으로 연결하여 원문을 입력하면 전기적 연결에 의해 새로운 암호문을 출력하는 방식으로 이 기계가 존재하지 않으면 암호를 풀 수 없다.

현대 암호

현대 암호는 1970년대 후반 스탠퍼드 대학과 MIT 대학에서 시작되었다. 1976년 스탠퍼드 대학의 Diffie와 Hellman은 '암호의 새로운 방향(New Directions in Cryptography)'이라는 논문에서 처음으로 공개키 암호의 개념을 발표하였다. 종래의 관용 암호 방식 또는 대칭키 암호 방식에서는 암호화키와 복호화키가 동일한 비밀키를 사용하기 때문에 송신자와 수신자는 비밀 통신을 하기 전에 비밀키를 공유하고 있어야 한다. 반면 공개키 암호 방식에서는 하나의 쌍이 되는 공개키와 비밀키를 생성하여 암호화에 사용되는 공개키는 공개하고, 복호화에 사용되는 비밀키는 사용자가 안전하게 보관하도록 한다. 공개키 암호 방식에서는 송신자와 수신자가 사전에 키를 공유할 필요가 없기 때문에 불특정 다수 사용자 간에 사전 준비가 없이도 암호 통신망을 구축하는데 유용하게 사용할 수 있다. 이어 1978년 MIT 대학의 Rivest, Shamir, Adleman은 소인수 분해 문제에 기반을 둔 RSA 공개키 암호를 개발했는데, 이것은 오늘까지도 가장 널리 사용되는 공개키 암호 방식이다. 공개키 암호의 도입은 현대 암호의 발전에 중요한 계기가 되었다.

한편, 1977년 미국 상무성 표준국(NBS, 현 NIST)은 전자계산기 데이터 보호를 위한 암호 알고리즘을 공개 모집하여, IBM 사가 제안한 DES (Data Encryption Standard)를 표준 암호 알고리즘으로 채택했다. DES의 표준화를 계기로 하여 금융 시스템을 중심으로 상업용 암호화의 이용이 증가하게 되었고 컴퓨터 통신망을 이용한 문서 전송, 전자 자금 이체 등이 활성화되었으며 암호 방식이 일반인들에게 알려지고 널리 사용되는 계기가 되었다.

이전의 암호 방식에서는 사용하는 키 뿐만 아니라 암호 알고리즘도 비밀로 하여 암호문의 비밀을 지키려고 하는 경우도 있었으나, 현대 암호에서는 암호 알고리즘을 공개하도록 하고 있다. 1883년 Auguste Kerckhoff는 암호 시스템의 안전성에 대해 '키 이외에 암호 시스템의 모든 것이 공개되어도 안전해야 한다'고 했는데 이것을 Kerckhoff's principle이라고 한다.

현대 암호

이렇게 함으로써 암호 방식의 안전성을 공개적으로 검토하게 하여 안전성을 확인하는 것이다.

표준화된 암호와 표준화된 컴퓨팅 기기들을 사용하는 현대 암호에서는 암호 알고리즘을 감추기가 매우 어렵다. 또한 암호 알고리즘을 감춘다고 해서 암호의 보안성이 높아지는 것도 아니다. 비밀로 다루어진 암호 알고리즘이 일단 공개되고 나면 그 안전성에 문제가 발견되는 사례가 많다. 그러므로 암호 분야에서는 어떤 암호 알고리즘이 많은 암호 학자들에 의해 장기간 세부적으로 수행된 분석에서도 잘 견디어 낼 때까지는 그 알고리즘을 안전하다고 인정하지 않는다. 즉, 암호 체계는 '무죄가 증명될 때까지는 유죄'이다.

암호체계의 분류

암호체계는 일반적으로 아래의 3가지 단계에 따라 유형을 분류한다.

- 평문을 암호문으로 변환하는 방식: 모든 암호 알고리즘에서는 평문을 암호문으로 변환하는데 두 가지 원리를 따른다. 즉 평문의 각 요소를 다른 요소로 바꾸는 대체(Substitution)이고 요소의 순서를 재조정하는 치환(Transposition)이다. 이 두 원리를 적 용하는데 있어 핵심은 어떤 정보도 손실되지 않아야 한다는 것이다.

- 사용된 키의 수(The number of keys used): 송수신 양단에서 같은 키를 사용하면 대칭 키 암호, 단일 키 암호, 비밀 키 암호, 또는 관용 암호라 부른다. 만일 송수신 양단에서 각자 다른 키를 사용하면 비대칭 암호 또는 공개 키 암호라 부른다.

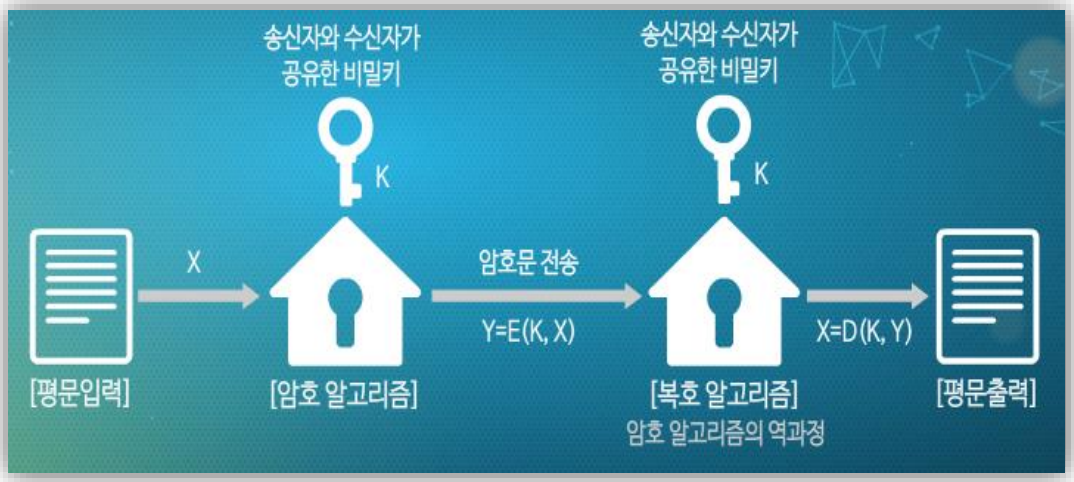
- 평문이 처리되는 방식: 블록 단위로 입력되고 출력되면 블록 암호(Block cipher), 비트 단위로 입력되고 출력되면 스트림 암호(Stream cipher)라고 부른다.

따라서 현대암호는 크게 대칭암호와 비대칭암호로 유형을 분류하며, 다시 대칭암호는 평문이 처리되는 방식에 따라 스트림암호와 블록암호로 분류한다. 비대칭암호에는 공개키 암호와 해쉬함수 등이 포함된다. 본 차시에서는 블록암호, 공개키 암호 및 해쉬함수에 대해서 자세히 학습한다.

02. 암호방식별 이해와 응용

대칭키 암호

- 대칭키 암호(비밀키 암호)는 암호화와 복호화 알고리즘에 동일한 키가 사용되는 방식의 암호 알고리즘을 말한다. 복호화에 사용되는 키는 제삼자에게 알려지면 안 되므로 송신자와 수신자는 사용되는 키를 비밀리에 공유하고 안전하게 보관해야 한다. 대칭암호 방식의 보안은 알고리즘의 비밀보다는 키의 비밀 유지 여부가 중요한 것이다. 이러한 대칭키 암호에는 스트림 암호와 블록 암호가 있다.



- **스트림 암호**

  스트림 암호는 대칭키 암호의 하나로 블록 크기를 1비트로 하여 블록마다 각각 다른 키를 사용하여 암호문을 생성하는 것으로 볼 수 있다. 암호화와 복호화 시 키스트림 생성기를 이용하여 키스트림을 생성하며, 이것을 평문과 연산하여 암호화하고, 거꾸로 이것을 암호문과 연산하여 평문을 얻어낸다. 즉, 스트림 암호는 바이너리 평문 스트림과 키스트림 수열의 XOR 연산으로 암호문을 생성한다.

  스트림 암호는 1970년대부터 유럽을 중심으로 발달하였는데, 안전성과 관련한 수학적 분석이 가능하고 알고리즘 구현이 쉬운 특징이 있어 군사 및 외교용으로 많이 사용되었다. 특히 구현 여건이 제약되는 이동 통신 환경에서도 구현이 용이하여 무선 데이터 보호에 많이 사용되었다. 대표적인 스트림 암호 알고리즘으로는 A5/1, A5/2 및 A5/3 등이 있는데, 각각 OECD에 가입된 유럽 국가에서만 사용되는 알고리즘, OECD에 가입되지 않은 국가에서 사용되는 알고리즘, 및 A5/1과 A5/2의 안전성 취약을 보안한 알고리즘 용도로 사용되었다.

- **블록암호(Block cipher)**

  블록 암호는 가장 보편적인 대칭 암호 알고리즘으로, 암호화와 복호화 시 특정 크기의 블록 단위로 암호화와 복호화 연산을 하는 방식의 암호를 블록 암호라고 한다. 즉 평문 입력으로 고정 길이의 블록이 사용되고 평문블록과 같은 길이의 암호문 블록 출력한다.

- **블록암호(Block cipher)**

  각 블록의 암호화와 복호화에는 동일한 키가 사용된다. 예를 들어 DES 암호는 64비트의 블록 단위로 암호화된다. 현재 많은 분야에서 대부분 블록 암호체계를 사용하고 있다. 대표적인 블록 암호로는 DES(Data Encryption Standard), Triple DES, 및 AES(Advanced Encryption Srandard)가 있다.

- **DES(Data Encryption Standard)와 Triple DES**

  DES는 1970년 IBM Lucifer 암호기 근간으로 개발되어 1977년 미국 정부(NIST) 표준으로 채택되어 가장 널리 사용된 블록 암호 알고리즘이다. DES 알고리즘은 평문을 암호문으로 변화하는 블록 사이즈가 증가하면 보안성은 강화되나 암복화 속도가 감소한다. 또한 암호 키의 길이가 길면 보안성 강화되지만 속도는 감소하여 키의 길이는 64나 128 비트가 적정하다.

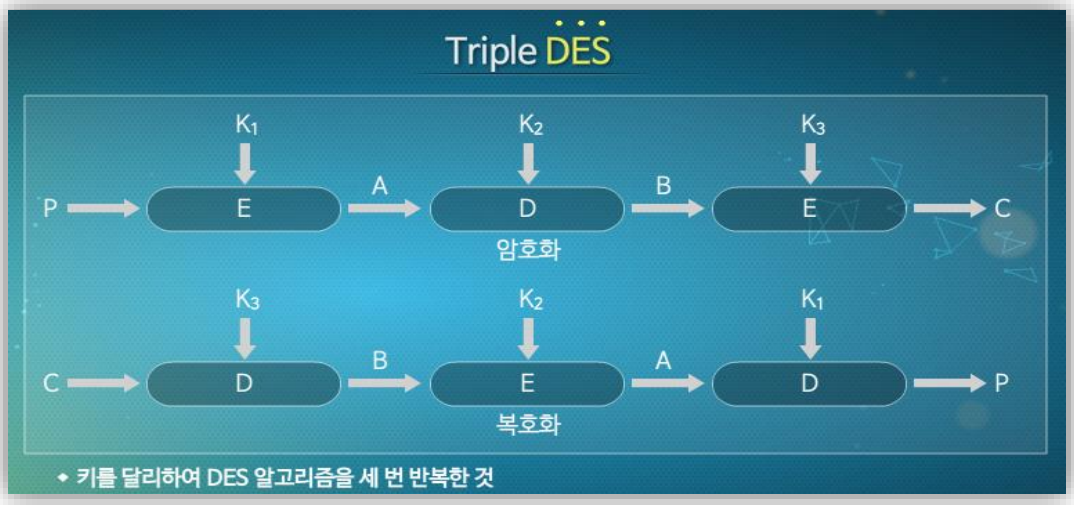
  미국 정부 표준으로 채택된 이후 20년간 사용되던 DES 알고리즘은 점차 약점을 노출하게 된다.

  - 1997년 2월 RSA사에서는 DES Challenge I 을 개최한 결과 78,000대의 컴퓨터를 병렬 연결하여 96일 만에 DES의 키를 찾는데 성공한다.

  - 1998년 7월에 DES Challenge II 가 개최되었는데 25만 달러의 전용 프로세서를 이용하 여 56시간 만에 키가 해독된다.

  - 1999년 1월에는 DES Challenge III에서 10,000대 컴퓨터 등의 컴퓨팅을 이용하여 22시 간 15분 만에 DES의 키가 해독된 것이다.

  이것은 DES가 표준 블록 암호 알고리즘으로서의 생명 종료를 시사하는 것이었고, 이를 근거로 새로운 블록 암호 표준 AES의 개발 사업이 이어지게 된다. 여기서 Triple DES알고리즘이 등장하게 되는데 이는 DES의 복호화가 가능해짐에 따라 새로운 암호체계 개발 전까지 임시로 사용한 암호화 알고리즘으로서의 역할이었다. 즉, Triple DES에서는 키를 달리하여 DES 알고리즘을 세 번 반복한 것으로 이해하면 된다(아래그림 참조).



◆ 키를 달리하여 DES 알고리즘을 세 번 반복한 것

ES(Advanced Encryption Standard)

1997년 미국 상무성(NIST)은 새로운 암호 알고리즘인 AES에 대한 제안요청을 공모하였다. 그 내용은

- 향후 30년 이상 사용 가능한 안정성
- 3DES 이상의 보안강도를 가지며 월등히 개선된 효율성
- 블록길이 128비트, 키 길이 128, 192, 256 비트 지원
- 평가항목: 보안, 계산 효율성, 메모리 요구량, H/W와 S/W 적합성, 유연성

공모에 따라 벨기에의 암호학자인 레인달(Rijndael)의 알고리즘이 선정되었고 2001년 1월 미국 NIST는 최종 선택안을 발표하였다. 참고적으로 암호키를 찾기 위해 암호키 모두를 검수하는데(brute-force) 소요되는 평균 시간을 아래의 표에 나타내었다.

키길이 (비트)	암호 방식	키 개수	초당 10^9 복호화 시 소요시간	초당 10^{13} 복호화 시 소요시간
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55}ns = 1.125년	1 시간
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127}ns = 5.3×10^{21}년	5.3×10^{17}년
168	3DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167}ns = 5.8×10^{33}년	5.8×10^{29}년
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191}ns = 9.8×10^{40}년	9.8×10^{36}년
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255}ns = 1.8×10^{60}년	1.8×10^{56}년

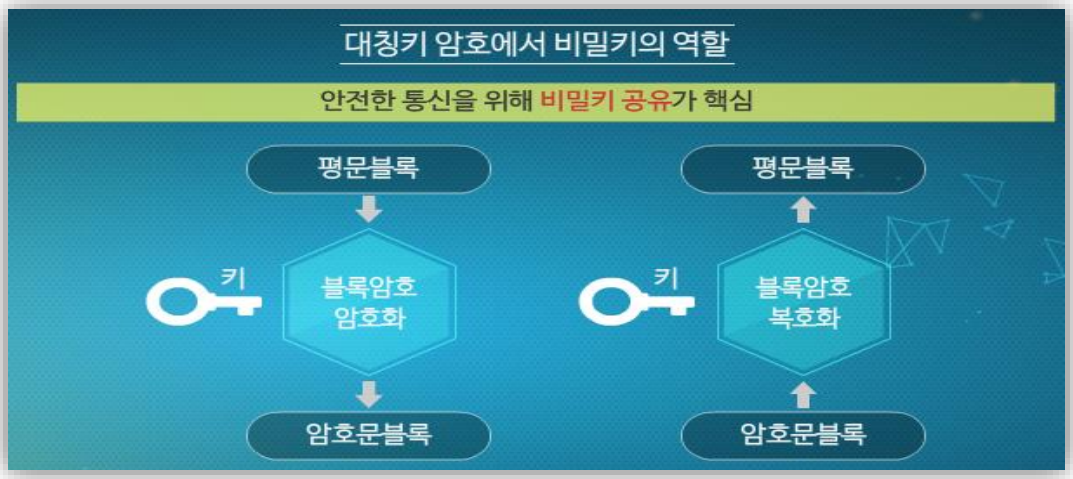
국내의 블록 암호 알고리즘

국내의 대표적인 블록 암호 알고리즘인 SEED 알고리즘은 1999년 2월 KISA(당시 한국정보보호진흥원)와 국내 암호 전문가들이 순수 국내 기술로 개발한 것이다. 128-비트 블록 암호로 전자상거래, 금융, 무선통신 분야에 널리 활용되고 있다. 1999년 9월 정보통신단체표준(TTA)으로 제정되었고 2005년에는 국제 표준화 기구인 ISO/IEC 국제 블록 암호, IETF 표준으로 제정되었다. 또한 2009년에는 256-비트 비밀키를 지원하는 SEED 256이 개발되어 그 활용성이 강화되었다.

ARIA 알고리즘은 국내의 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요하여 국가보안기술 연구소(NSRI) 주도로 학계, 국가정보원 등의 암호전문가가 개발한 국가 암호화 알고리즘이다. 경량 환경에서의 효율성 향상을 위해 개발된 128비트 블록 암호 알고리즘으로 2004년 국가표준기본법에 의거 국가표준(KS)으로 지정된 바 있다.

비대칭키 암호

- 대칭 암호화 알고리즘은 메시지 암호화 때 사용했던 대칭 키를 보내지 않으면 복호화 불가하기 때문에 양측이 안전하게 통신을 하기 위해서 비밀키를 공유하는 것이 핵심이다. 대칭 암호를 사용하기 위해서는 키를 사전에 건네주는 키의 배송 문제(key distribution problem)를 해결해야 하는 것이다. 하지만 대칭키 사용자의 수가 많아지면 통신을 위한 키의 수가 N(N-1)/2개로 N의 증가에 따라 기하급수적으로 방대해지는 문제가 발생한다.



- **공개키 암호**

  공개 키 암호 방식은 대칭의 키 배송 문제를 해결한 방식이다. 하나의 쌍이 되는 두 개의 키를 생성하여 하나는 암호화에 사용하고 다른 하나는 복호화에 사용한다. 암호화에 사용하는 키는 공개할 수 있어서 공개키라고 부르고, 복호화에 사용하는 키는 사용자만이 안전하게 보관해야 하므로 개인키(비밀키)라고 부른다. 두 개의 키가 서로 다르므로 비대칭키 암호라고 부르며, 하나의 키를 공개하므로 공개키 암호라고도 부른다.

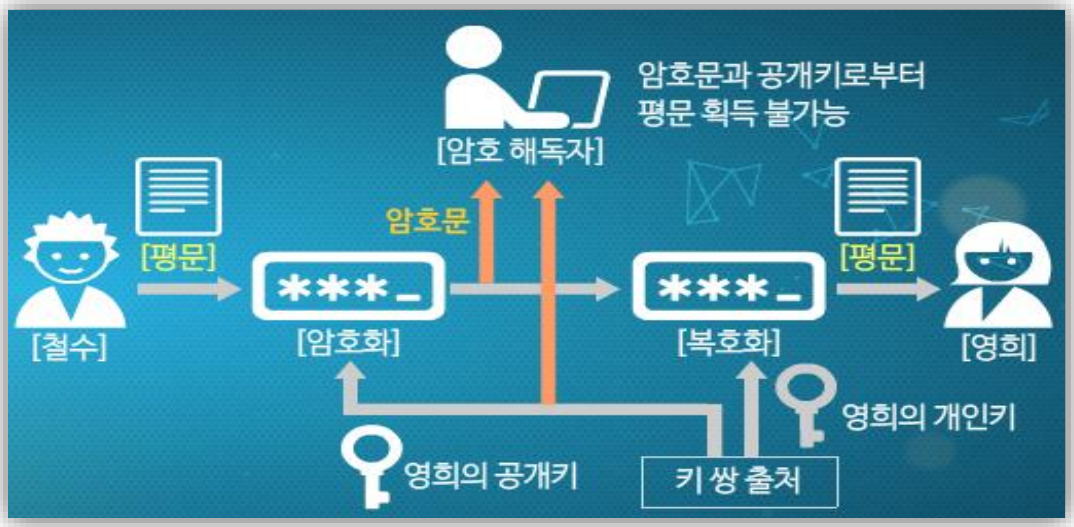
[공개 키: 두 개의 키를 사용하는 암호 시스템]

- 공개키 사용 유형은 개인키와 공개키의 적용방식(그림 11)에 따라 그림 12에 도시한 것과 같이 암호화/복호화(기밀성 제공), 디지털 서명(인증 및 부인방지) 및 키 교환으로 구분한다.

[공개키와 개인키의 사용]

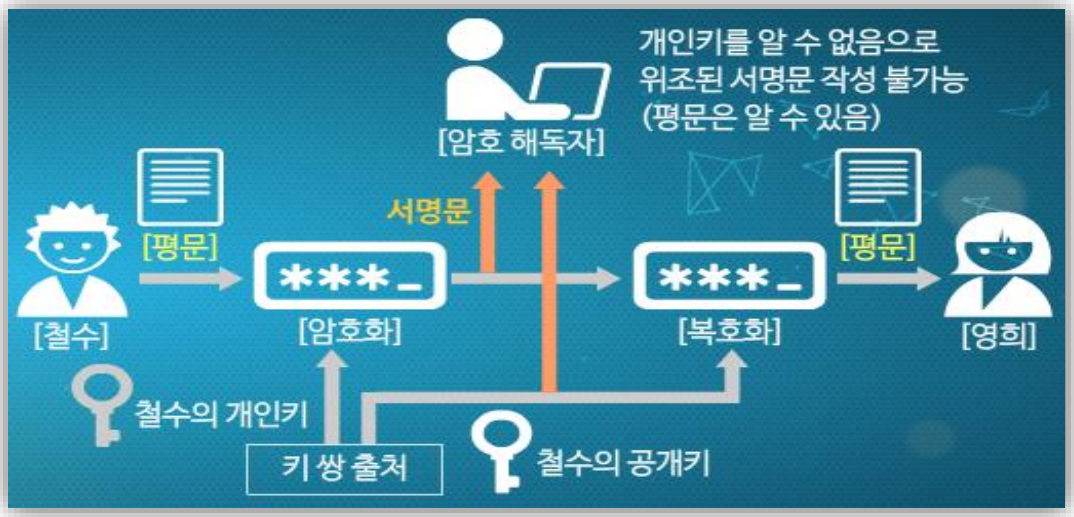
[공개키 사용 유형]

- 공개키 암호 알고리즘의 가장 기본적인 기능은 기밀성(Confidentiality)의 제공이다. 예를 들어 철수는 영희의 공개키(Public Key)를 이용해 암호화하여 전송하면 영희만이 자신이 가진 개인키(Private Key)를 이용해 철수의 편지를 복호화할 수 있어 기밀성을 제공할 수 있게 된다.



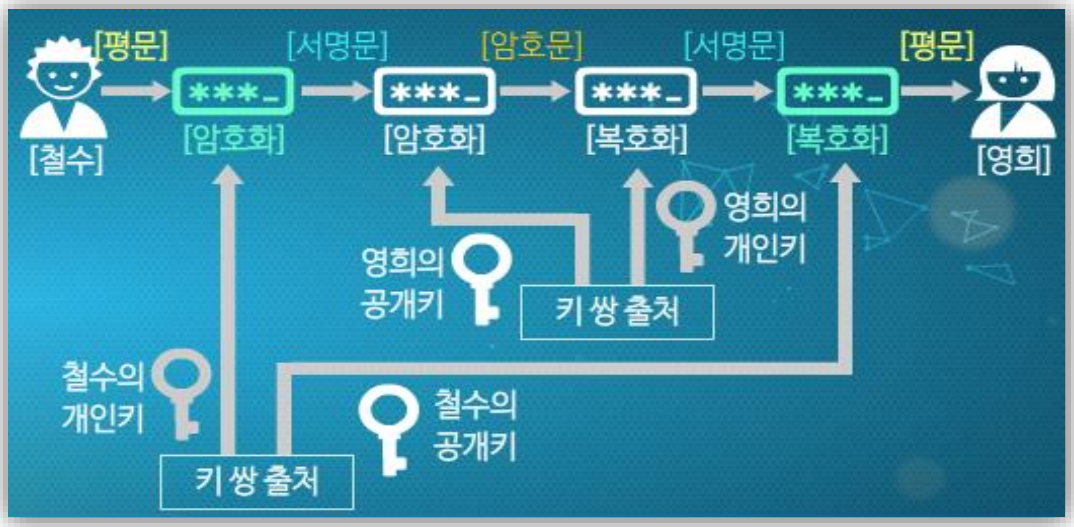
[공개키를 이용한 기밀성 제공]

- 인증 기능 및 부인방지 기능을 제공하는 디지털 서명은 개인키로 서명함으로써 송신자 인증을 제공할 수 있다. 예를 들어 그림 14과 같이 철수는 영희에게 편지를 전송하는데 철수의 개인키로 편지를 암호화하여 전송하면 영희는 철수의 공개키로 복호화하여 철수가 보낸 편지임을 확인할 수 있다.



[개인키를 이용한 디지털 서명 기능]

- 한편 개인키로 서명하고 공개키로 암호화하여 인증 기능과 기밀성을 동시에 제공할 수 있다. 철수는 자신의 개인 키로 암호화하여 서명문을 생성하고 그 서명문을 영희의 공개키로 암호화하여 암호문을 생성하므로써 영희는 자신의 개인키로 서명문을 복호화하고 철수의 공개키로 철수 보낸 편지 임을 확인할 수 있다.



[기밀성과 인증 기능 제공]

- **대칭키와 공개키 암호 방식의 비교**

  공개키(public key) 암호의 주요 장점은

  - 강화된 보안성과 편리함
  - 전자서명 기법을 제공: 부인방지 (NonReputation)
  - 사용자가 스스로 자신의 개인키 보호에 대한 전적인 책임

  공개키 암호의 주요 단점으로는

  - 공개키 암호는 대칭키에 비해서 훨씬복잡

  . 공개키 암호를 대형 파일을 암호화하는데 부적합

  . 대칭키 암호로 암호화하고 대칭키는 공개키로 암호화하여 전송하는 방식을 적용

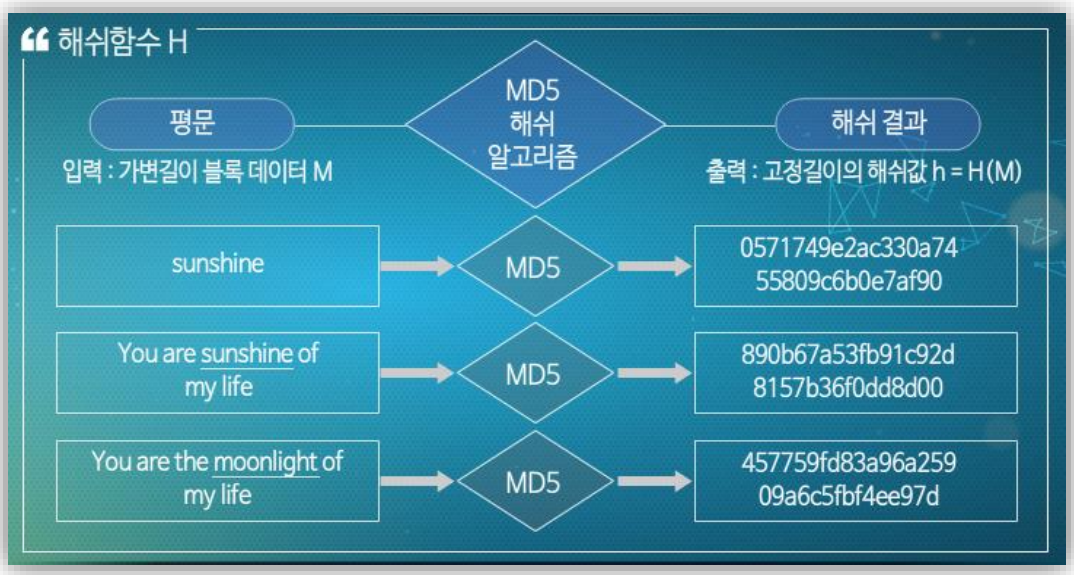
  - 가장 공격(Impersonation)에 취약: 인증기관 공격으로 획득한 공개키 인증서를 사용해 다른 사용자로 가장

해쉬함수(hash function)와 그 응용

- 해쉬함수는 임의 길이의 문자열을 고정된 길이 문자열로 매핑하는 메시지를 기초로 하는 일방향 함수이다. 해쉬함수의 결과은 해쉬값, 메시지 다이제스트, 메시지 지문라고 불린다.

[해쉬함수]

- 해쉬함수의 요구사항으로는 메시지 길이에 관계없이 일정 길이 해쉬 값 출력해야 한다. 예를 들어 그림 17과 같이 길이가 다른 세 평문의 경우 길이가 같은 32개 문자의 해시 결과를 발생시킨다.



[임의 문자열에 대한 동일 길의 해쉬 값 출력]

- 따라서 해쉬함수는 입력정보에 대해 변조할 수 없는 특징 값을 나타내기 때문에 통신 중에 정보의 변조가 있었는지 여부를 확인하는 용도로 사용된다. 이런 용도로 사용될 수 있기 위해서 해쉬함수는 같은 해쉬값을 가지는 두 개의 입력 메시지를 찾는 것이 계산적으로 불가능해야 한다. 따라서 해쉬함수의 특성을 활용하여 해쉬함수는 메시지 인증(Message Authentication), 전자서명 (Digital Signatures), 소프트웨어의 변경 검출, 일방향 패스워드 파일 생성, 침입탐지나 바이러스 탐지 등에 응용되어 사용되고 있다.