Week 12.

Network Security

Network Security

- 안전한 통신이란?
  - Confidentiality(기밀성) : 송신자와 송신자가 의도한 수신자만 이 내용을 이해할 수 있어야 함.
  - Message Integrity : 보내는 사람&받는 사람이 내용이 변하지 않았다는 것을 보장할 수 있어야 함.
  - End-Point Authentication : 송신자나 수신자가 자기의 정보(신원)을 밝혔을 때, 그 사람이 맞다는 것을 확신할 수 있어야함.
  - Operational security : 운영상의 보안. DNS를 접근 할 수 있는 권한을 믿을 수 있는 사용자 몇 에게만 허용을 해야함.

Network Security

- 통신을 위협하는 것들
  - Eavesdrop : 엿듣기, 각종 개인정보를 가로채 갈 수 있다.
  - Impersonation : 자신의 IP주소를 바꿔서 마치 자신이 다른 사람인 양 공격함. 가장 공격.
  - Hijacking : 통신하는 두 주체 사이에 전달되는 정보를 가로채거나 대신 자신의 정보를 넣는 것.
  - DoS : 서비스 거부 공격. 정당한 서버에 허위 메시지를 보내서 동작하지 못하도록 함.
  - 기타 운영보안(Operational Security)에서 허용되지 않은 사람외에 나머지는 다 bad guy 임.

Cryptography Principles

- 용어정리
  Plain text : 평문. 원래 보내려는 메시지
  Cipher text : 암호문. 암호화된 메시지
  Encryption Algorithm : 암호화 알고리즘.
  Decryption Algorithm : 복호화 알고리즘
  m : 평문 / $K_A(m)$: A라는 알고리즘으로 암호화한 암호문
  $K_B(K_A(m))$: 그걸 다시 B라는 키로 복호화 한 것 (= 평문)

  - Substitution Cipher

    - 대치하는 암호화 알고리즘. (a는 e로 쓰고, b는 h라고 쓰도록 정해 놓듯이 특정 알파벳을 뭐라고 쓸지 규정 지어놓고 그거에 맞춰서 씀.)

    - 해독되기 쉬움. (q나 z는 영어에서 사용빈도 수가 적기 때문에 뭐가 q나 z인지 알 수 있음.)

Cryptography Principles

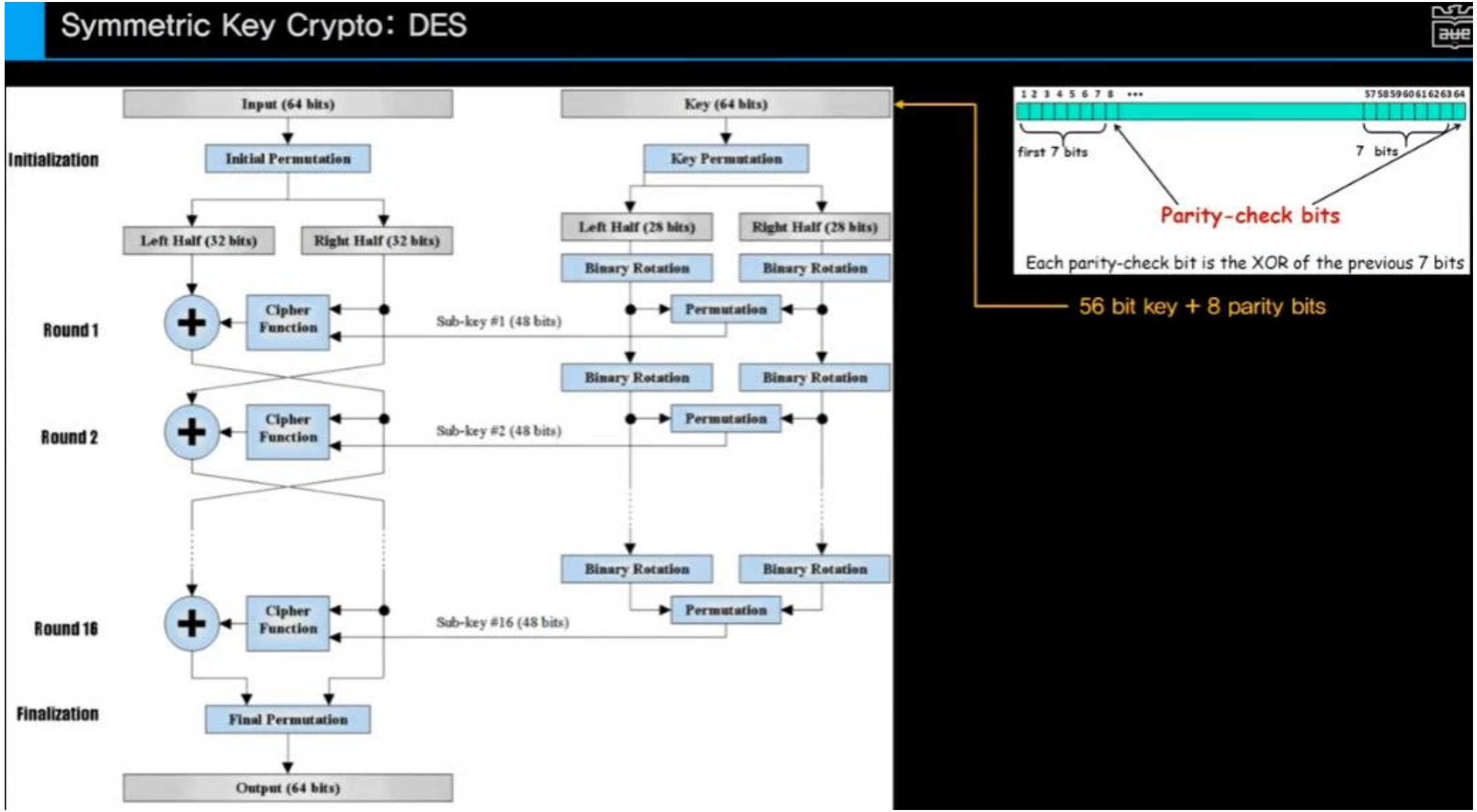
- 암호화 알고리즘은 크게 Symmetric Key Cryptosystem (Secret key System) 이랑 Asymmetric Key (Public key System) Cryptosystem으로 나누어짐.

- Symmetric은 암호화랑 복호화에 쓰는 키가 같음. 그래서 대칭 키 알고리즘. 키는 주체끼리만 알고있어야 함.

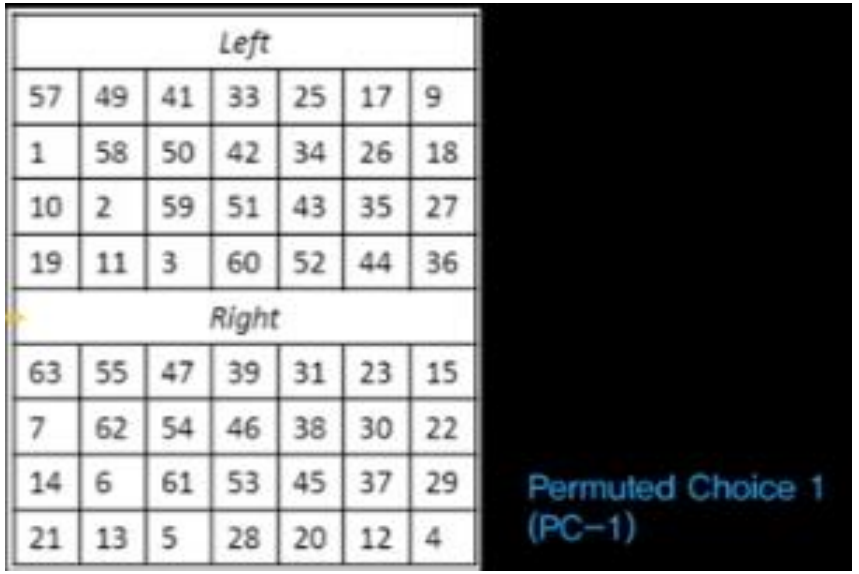
- Asymmetric은 암호화랑 복호화에 쓰는 키가 다름. 그래서 비대칭 키 알고리즘. 키 하나만 자신이 가지고, 다른 키는 공유해도 됨.

- Symmetric Key Cryptosystem
  - 송신자가 $K_S(m)$ 이렇게 메시지를 보내면, 수신자가 $K_S(K_S(m))$ 이렇게 해독해서 확인함.
  - 키 내용을 어떻게 서로 공유할 것인지가 문제점. 온라인으로 공유하면 탈취 위험 있음.
  - DES (Data Encryption Standard)가 중요한 알고리즘.

Cryptography Principles



Cryptography Principles



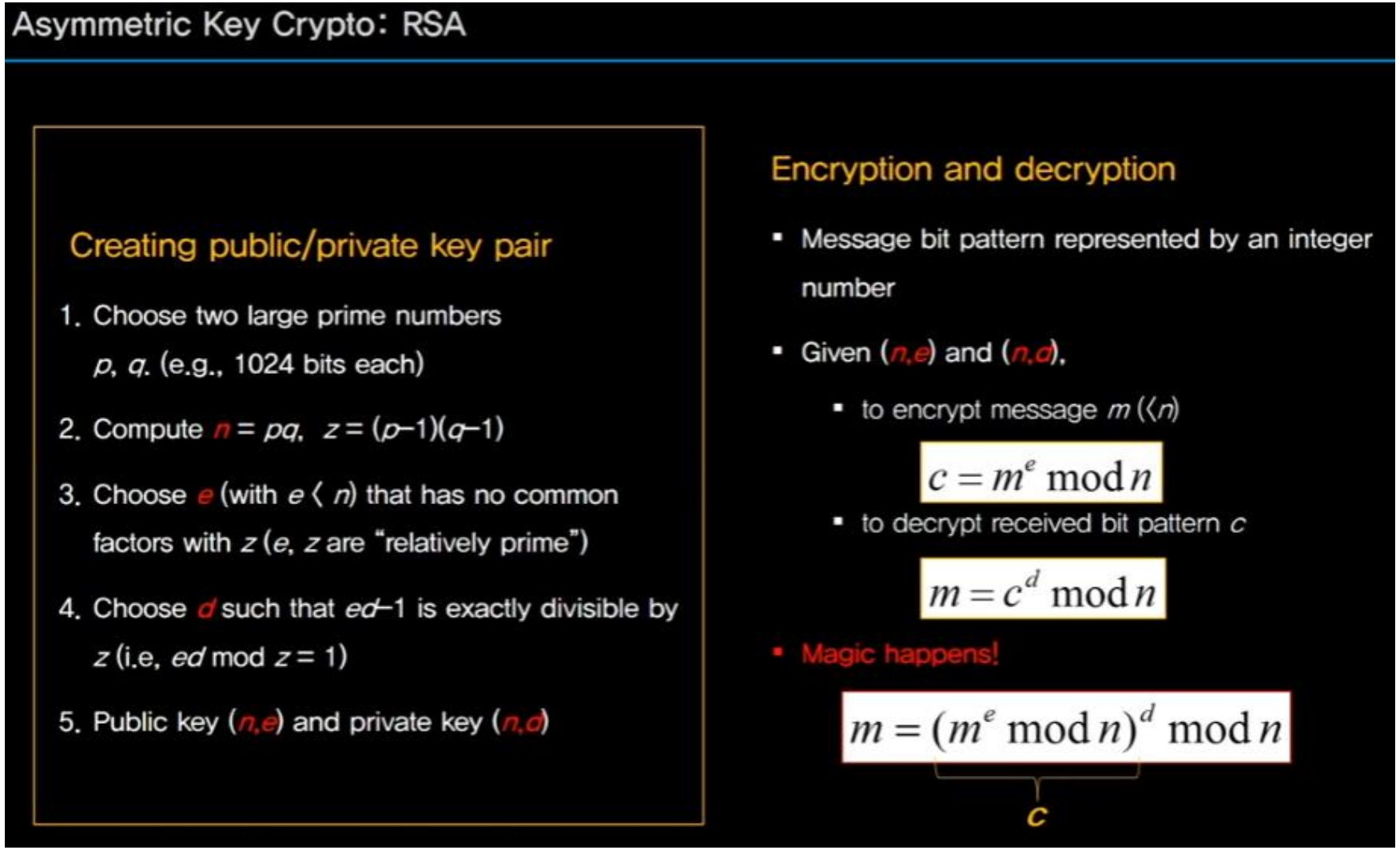
- Key permutation에는 이 표가 사용된다.
- Binary rotation 을 하면 57이 우측 하단으로 넘어가고, 49부터 앞으로 한 칸 당겨진다. 두 칸 당겨질 수도 있다.
- 예전의 컴퓨터 사양으로는 키를 모르는 상태에서 plain text 찾기가 힘들었다. 그런데 1990년대 말에 컴퓨터의 연산속도가 빨라지면서 DES는 점점 사용하지 않게 되었다. 그래서 3DES (DES를 세번하는 것) 라는 아이디어가 나왔고, 그 뒤 AES가 제안되었다.
- AES(Advanced Encryption System) : DES의 두 배의 길이의 블록단위로 암호화를 하는 것. 키에 대한 사전 정보 없이 brute-force로 뚫으려고 하면 149조 년이 걸림.

Cryptography Principles

- Asymmetric key Algorithm
  - 통신의 두 주체가 서로의 비밀키를 공유할 필요가 없음.
  - 두 주체는 퍼블릭 키, 시크릿 키 한 쌍을 가짐.
  - 대표적으로 RSA가 있다.
    - 두 개의 매우 커다란 소수를 찾고, 그 두 수를 곱한 값 n을 계산한다.
    - 그리고 소수에서 각각 1을 뺀 값을 n에 곱해 z를 얻어낸다.
    - 그 다음 암호화에 퍼블릭키로 사용할 e 와 복호화에 사용할 프라이빗 키 두 개를 만들기 위해 e와 d를 찾는데 e와 d는 z와 서로소인 소수다
    - 암호화에 사용하는 퍼블릭키는 n, e / 복호화에 사용될키는 n, d 한 쌍임.
    - 만약 시크릿 키를 공유할 때는 내 시크릿 키를 상대방의 퍼블릭 키로 암호화 해서 보내고, 상대방은 자신의 프라이빗 키를 가지고 그것을 복호화해서 공유할 수 있다.

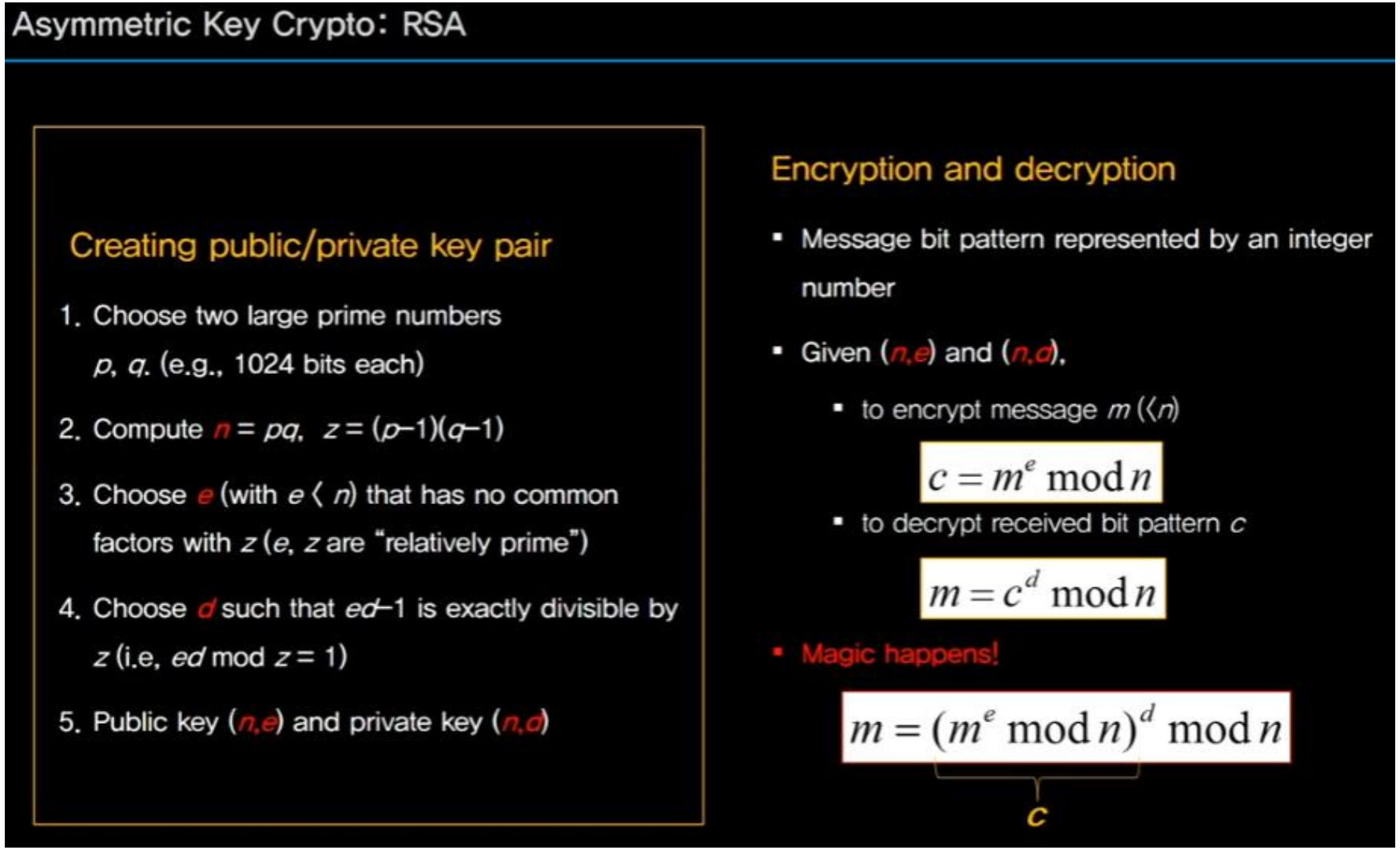
Cryptography Principles

- Asymmetric key Algorithm



Cryptography Principles

- Asymmetric key Algorithm



Message Integrity

메시지 무결성을 제공하려면 두 가지가 보장되어야 한다.

1. 보낸 사람이 진짜 Alice가 맞다.
2. Bob에게 오는 과정에서 메시지가 변질되지 않았다.

이것을 할 수 있는 방식으로는 두 가지 방법이 있다.

- MAC (Message Authentication Code)
- Digital Signature

Message Integrity

- MAC (Message Authentication Code)
  - Ver 1
    - 메시지 m을 해시 함수를 거쳐서 H(m)으로 만들고 m과 H(m)을 수신자에게 보낸다.
    - 수신자는 m을 해시 함수를 거쳐서 H(m)값이 나오는지 확인한다.

만약 trudy가 m을 변질시킨 m`, 이를 해시 함수를 적용한 H(m`)으로 바꿔서 (m`,H(m`))을 수신자에게 보내면 수신자는 이를 구별할 방법이 없으므로 안전하지 않다.

그래서 통신의 두 주체간 시크릿키를 서로 알고 있다는 전제 하에 ver 2가 나왔다.

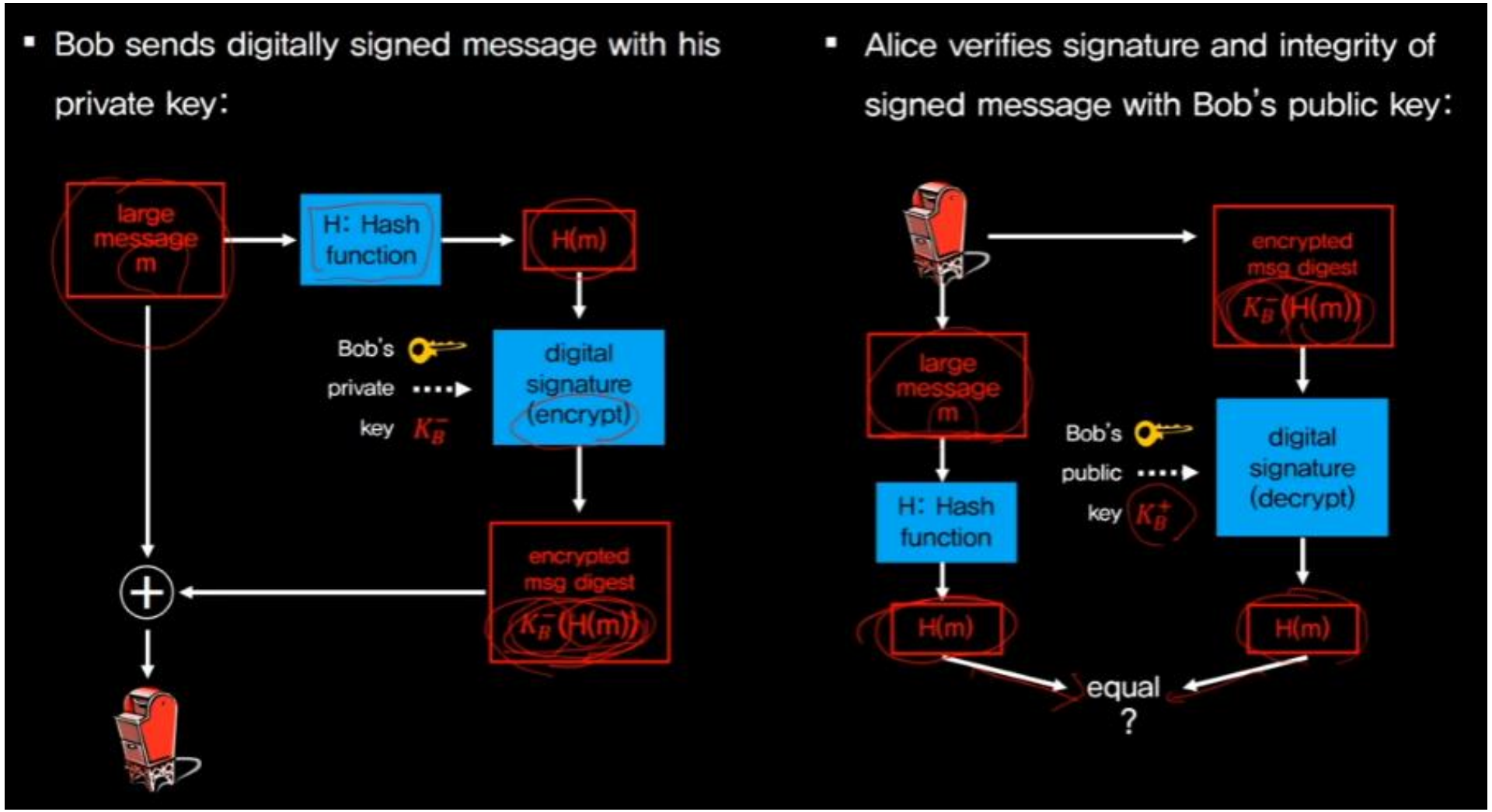
  - Ver 2 (Trudy는 송, 수신자의 시크릿키 s를 모르기 때문에 ver2는 안전하다.)
    - 송, 수신자는 서로의 시크릿 키 s를 알고 있다.
    - 원래 메시지 m에 s를 더해서 m+s를 해시 함수를 적용시킨다.

Message Integrity

- 전자서명
  - ‘개인 키, 공개 키가 한번 씩만 적용이 된다면, 어떤 순서로 적용되든지 결과는 똑같다.’라는 특성에 기반한 것.
  - Bob이 메시지의 해시값 H(m)을 개인키를 통해 암호화 해서 Alice에게 전달함.
  - Alice는 원문 m과, 암호화된 해시값을 받음.
  - M에 해시함수를 적용시킨 H(m)과 암호화된 해시값을 Bob의 공개키로 복호화를 해서 H(m)이 나오는지 확인한다.

Message Integrity

- 전자서명



End-Point Authentication (통신 개체의 인증)

- 가장 많이 쓰이는 방식은 패스워드를 전달하는 방식
- 그러나 이는 Trudy로 하여금 Playback attack(replay attack)이라는 허점을 제공할 수 있다.
- Playback attack은 Alice가 보내는 메시지를 통째로 탈취해서 캡쳐해놓는 방식의 공격.
- 메시지가 암호화 되어있는지는 중요하지 않고 그냥 그 메시지를 통째로 탈취해서 전달하는 공격방식이기 때문에 본인이 Alice인 척 행세를 할 수 있다.

➔ 그래서 이를 막기 위해 Nonce 라는 것이 도입 됨.

End-Point Authentication (통신 개체의 인증)

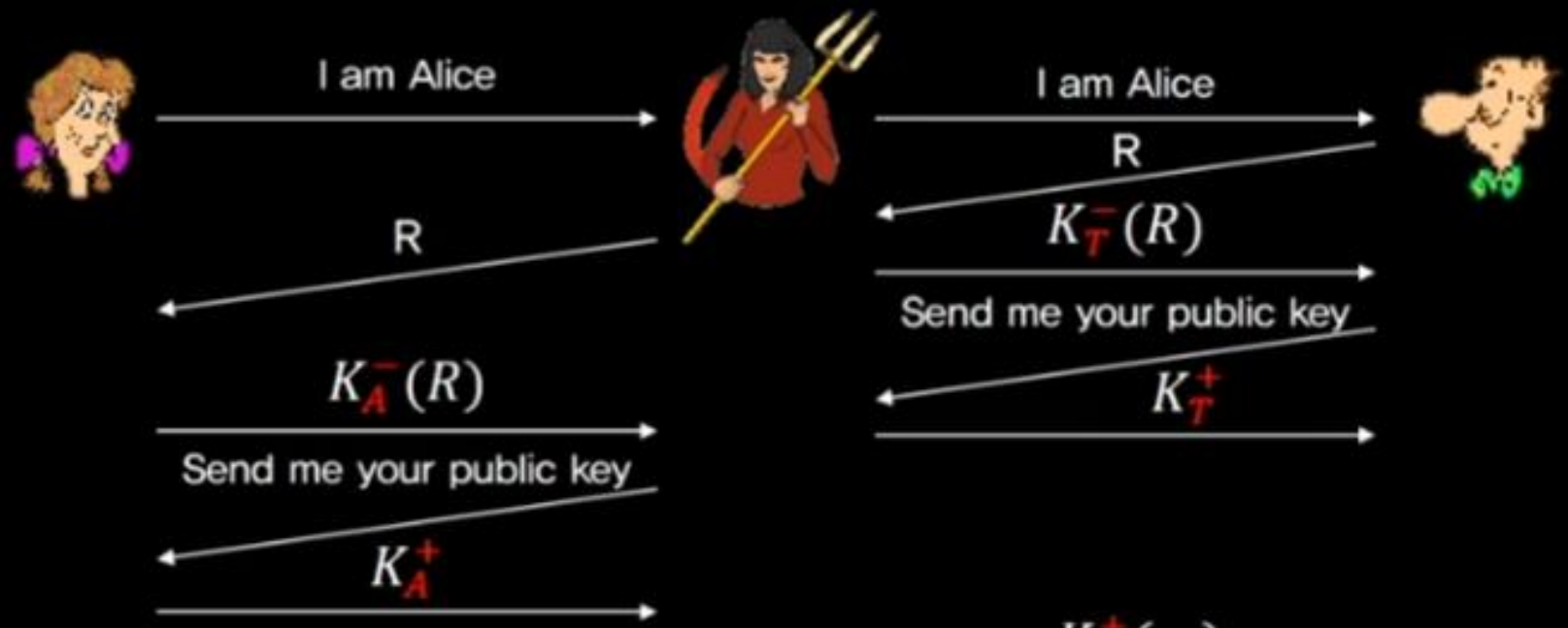
- Nonce
  - 굉장히 큰 숫자 중 랜덤하게 만들어지는 숫자.
  - Alice가 서버에게 자신이 Alice임을 알리면 서버는 위의 랜덤한 숫자 R을 부여받는다.
  - R을 Alice와 Bob만이 알고있는 공통의 secret key로 암호화 한다.
  - 매번 접속 때마다 다른 숫자 R을 공통의 암호키로 암호화 했다면 서로임이 인증된다.
    - 하지만 이 역시, 서로가 secret key를 공유하고 있어야 한다는 문제점이 있다.

End-Point Authentication (통신 개체의 인증)

- Nonce 2nd version
  - Bob이 Alice에게 R을 보내면, Alice가 자신의 시크릿 키로 R을 암호화해서 Bob에게 보낸다.
  - Bob는 Alice의 공개 키로 이를 복호화 해본다.
  - 그랬을 때 자기가 보낸 R이 나오면, Alice가 답장했음이 인증된다.
    - 그렇지만 이 또한, Trudy가 man-in-the-middle attack을 할 수 있다.

End-Point Authentication (통신 개체의 인증)

- Man–(or Woman)–in–the–middle–attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



End-Point Authentication (통신 개체의 인증)

이런 문제를 해결하기 위해서 나온 것이 인증 기관(Certification authority) 이다.

1. Alice/Bob이 인증기관에 가서 자신의 신분증을 보여주고 퍼블릭 키를 발급 받는다.
2. 그 퍼블릭 키를 인증 기관에 등록한다.
3. 인증 기관은 그 퍼블릭 키를 인증 기관의 프라이빗 키로 암호화해서 공개한다.
4. Bob/Alice가 인증 기관의 퍼블릭 키로 해당 내용을 복호화 해서 Alice/Bob임을 믿을 수 있다.

Securing E-mail

1. 보내는 사람이 Alice라고 하면, Alice가 먼저 대칭 키를 생성하고 메시지를 그 대칭 키로 암호화한다.
2. 대칭 키를 Bob의 Public key를 사용하여 암호화한다.
3. Bob는 자신의 Private key로 복호화 해서 대칭 키를 얻고, 그 대칭 키로 메시지를 복호화한다.

IPsec and VPNs

IPsec : 네트워크 계층에서의 보안을 제공함. IP 데이터 그램의 암호화를 위한 프로토콜.

VPN (Virtual Private Network) : 인터넷 자체는 공용 네트워크를 사용하되 자신들의 정보를 공용 인터넷에 흘려 보내기 전에 암호화를 해서 논리적으로 분산 되어있는 네트워크로 만드는 것.

- IP sec의 종류
  - Authentication Header(AH)
  - Encapsulation Security Protocol(ESP)

둘 다 데이터 무결성은 제공하지만 AH방식은 데이터 기밀성은 제공하지 않음. 즉, 암호화하지 않고 데이터를 전송함. 그래서 주로 사용되는 것은 ESP 방식.

IPsec and VPNs

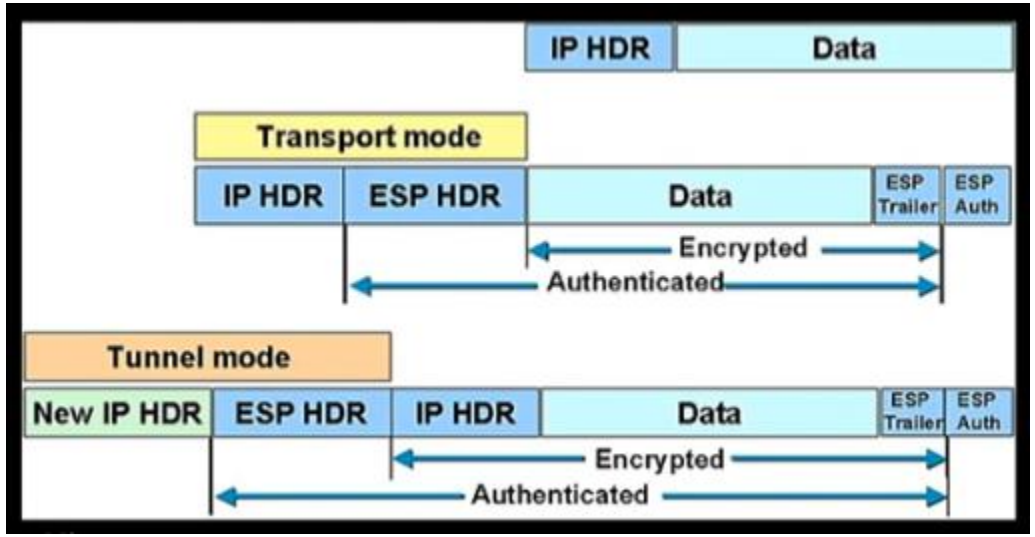
- ESP 프로토콜의 종류

  ■ Transport mode

  □ 두 호스트 간에 이루어짐. ESP 헤더와 데이터가 같이 Authentication이 됨.

  ■ Tunnel mode

  □ IP 헤더도 암호화 되고 새로운 IP 헤더가 붙음. 데이터가 어디로 가는지를 숨기기 위함. Tunnel 모드가 더 잘 쓰임.

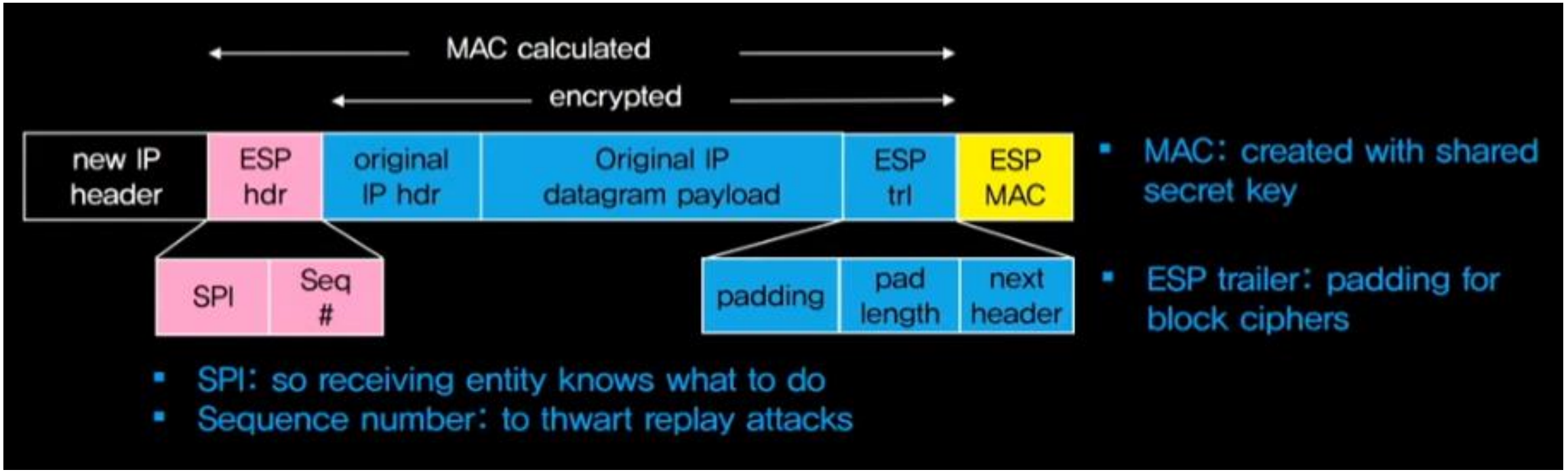


IPsec and VPNs

- Security Associations (SAs)
  - 한 방향으로 만들어지는 논리적 연결 그러므로 상호 연결을 위해선 두 개의 SA, 한 쌍이 필요함.
  - R1, R2는 모든 SA에 대해서 처리 방식을 알고 있음
    - Security Parameter Index (SPI) : 각각의 엔트리를 구별하는 Index
    - SPI가 붙어있는 송/수신 인터페이스의 IP 주소
    - 두 호스트 간의 어떤 암호화 기술을 사용하는지
    - 메시지 무결성을 체크하기 위한 MAC코드 등등
  - 이런 데이터들을 저장하는 곳이 Security Associations Database (SAD)다.

IPsec and VPNs

- ESP Tunnel Format



- ESP Trl은 암호화 알고리즘을 사용하기 위해 데이터를 64bits, 128bits의 정수배로 맞추기 위한 채우기 코드.
- 그리고 그 데이터를 Encryption하면서 SPI를(어떤 방식으로 암호화된 건지 수신자에게 알려주기 위함) 붙인다.
- ESP헤더에는 또한 sequence number도 포함된다. Replay attacks를 방지하기 위함이다.

IPsec and VPNs

- Internet Key Exchange(IKE) 프로토콜
  - 2단계로 이루어진다.
    1. 서로 인증을 하는 단계. Diffie-Hellman 알고리즘을 사용하여 퍼블릭 키를 만듦
    2. 어떤 암호화 방식을 쓰고 어떤 키를 사용할 것인지를 공유함.

Wi-Fi Security

기본적으로 무선은 유선보다 보안에 취약함.
그래서 나온 것이 Wired Equivalent Privacy (WEP) 그러나 보안 취약성 때문에 이제는 사용되지 않음.

- Wired Equivalent Privacy (WEP)
  - ■ 64비트의 키로 Key sequence generator가 만들어진다.
    - □ 40비트의 shared secret, 24비트의 Initialization Vector (IV) 값을 가지고 만들어짐
  - ■ 그러나 IV값마저 암호화를 거치면 수신자 측에서는 복호화 할 수 없으므로 IV는 Plain text로 전달 됨.
  - ■ 해커가 이미 잘 알려진 컨텐츠 Di와 IV를 통해 암호화된 컨텐츠 Ci를 Exclusive-OR 시키게 되면 암호화 시퀀스 Ki를 알 수 있다.

→ 그래서 제시된게 Wi-Fi Protected Access (WPA) 여기에 Pre-Shared Key (PSK)를 사용하면 WPAPSK 방식.

+) WPA는 RC4라는, 기존의 WEP과 똑같은 sequence generator를 사용하고
WPA2는 AES기술을 사용하여 훨씬 더 보안이 강화됨.

Wi-Fi Security

- 802.11i
  - Client station을 STA, Access Point를 AP, Authentication Server를 AS라고 한다.
  - STA과 AS 사이에 알아서 인증 키를 만들 수 있게끔 만들었음.
  - 작동순서

1. STA가 보안 소프트웨어를 다운받아 설치한다. 그러면 주변 AP를 찾는다.

2. STA가 AP를 통해서 AS에 접속한다. 이 때 공유키 방식의 인증을 통해서 상호 마스터 키를 만든다.

3. 이 마스터 키에 기반하여 실제로 적용할 쌍이 되는 Pairwise Master Key(PMK)를 양쪽에서 만든다.

4. AS가 AP에게 PMK를 전달함으로써 AP는 같은 PMK를 가지고 STA와 통신할 수 있게 됨.

Firewall and IDS:IPS

Header에 담겨있는 정보만을 가지고 어떤 동작을 하는 것을 firewall이라고 한다. 그런데 이는 보내는 쪽에서 주소를 바꿔서 보내게 되면 쉽게 통과할 수 있다. 그래서 IDS/IPS가 도입되었다.

IDS : Intrusion Detection System
IPS : Intrusion Protection System

- IDS/IPS는 헤더 정보만 이용하는 것이 아니라, 실제로 그 안에 담겨있는 payload 정보까지 읽어서 뭔가 의심스러운 패킷이다 싶으면 그것을 처리하는 것.

- IDS는 로그 메시지를 알리든지, 경보 메시지를 관리자한테 전달함 → 소극적
  IPS는 패킷을 스스로 차단시켜 버림 → 적극적

Firewall and IDS:IPS

- Firewall
  - Stateless packet filters
    - 중간의 라우터가 firewall 역할도 하는데 패킷 단위로 검증함.
    - Src 주소, dest 주소, 포트 번호를 가지고 drop or pass 를 결정하는 단순한 방식.
    - 그러다보니까 현재 상황은 파악하지 않은 채 조건만 맞춘 패킷은 그냥 받아들이게 됨 → DoS 공격에 매우 취약.
  - Stateful packet filters
    - 연결이 일어나면 커넥션 테이블에 이를 저장해놓고, 패킷을 받을 때마다 커넥션 테이블을 체크해서 실제로 유효한 연결인지 검사를 하고 통과시킴.

Firewall and IDS:IPS

- Firewall
  - Application gateways
    - 특정 응용서비스를 특정 사용자들에게 허락하는 데, 그 경우에 어플리케이션 게이트웨이를 통과하게끔 하는 방식.
    - 해당 게이트웨이를 통과하지 않은 트래픽은 전달되지 않음.
    - 내부 사용자들 중 특정 사용자만 외부로 telnet을 할 수 있도록 함.

- IDS/IPS
  - 패킷을 더 자세히 관찰함 (Deep Packet Inspection)
  - 여러 패킷들이 가지는 이상한 순서들도 발견할 수 있음.

Firewall and IDS:IPS

- IDS
  - 한 군데만 설치되는 것이 아니라 한 네트워크 내에서도 여러 군데 설치됨.
  - Payload 정보까지 살펴봐야 하기 때문에 한 군데에만 두면 오버헤드가 과하게 몰리게 됨.
  - 웹서버, FTP서버, DNS 서버 같은 경우 외부 사용자들에게 서비스하기 위해서 만들어졌기 때문에 IDS시스템을 강하게 적용하면 사용자들이 접근하지 못함.
  - 적용하더라도 DMZ에 배치함으로써 보안을 살짝 약화시킨다.

Firewall and IDS:IPS

- IDS Types
  - Signature-based system
    - 다양한 네트워크 어택에 대한 정보를 다 갖고 있음.
    - DB화 되어있는 공격은 빠르게 처리가 가능하나, DB화 되어있지 않으면 탐지 불가.
  - Anomaly-based system
    - 평소 동작 중에 스스로 트래픽을 관찰해서 프로파일을 만들어 놓음.
    - 일반적인 트래픽인지 네트워크 공격의 일종인지를 구별하는 것이 어려움.
    - DB화 되어있지 않은 공격도 탐지할 수 있으나 위의 문제 때문에 현재 머신러닝이나 딥러닝을 이용해보려는 연구들이 많이 이뤄지고 있음.

summary

- 기밀성(confidentiality): 허가된 송신자와 수신자만이 데이터를 읽을 수 있어야 함을 의미하는 보안 요구 사항
- 메시지 무결성(message integrity): 전송 중 데이터 내용이 변경되지 않았음을 보장해야 함을 의미하는 보안 요구 사항
- 엔드포인트 인증(end-point authentication): 데이터 송신자가 정말 자신이 주장하는 그 사람임을 보장해야 함을 의미하는 보안 요구 사항
- 평문(plaintext): 암호화 되지 않은 원래 문장
- 암호문(ciphertext): 암호화된 문장
- 대칭키 암호화(symmetric cryptography): 암호화와 복호화에 동일한 키를 사용하는 암호화 기술
- 비대칭키 암호화(asymmetric cryptography): 암호화와 복호화에 서로 다른 키를 사용하는 암호화 기술
- 전자서명(digital signature): 네트워크에서 전송되는 문서에 전자적으로 서명하는 기술
- 방화벽(firewall): 외부에서 들어오는 네트워크 공격을 막아주는 시스템
- 침입탐지시스템(Intrusion Detection System, IDS): 허가되지 않은 사람의 침입을 감지하는 시스템

감사합니다