CSE 겨울학교(A Basic CS skill, ABC)
멘토 활동 보고서

Intentionally deleted

10 차시 - Security and Cryptography

활동 개요

활동 날짜 : 2020.02.17.

활동 시간 : 20:00 ~ 21:00 (1시간)

활동 장소 : 온라인 (Microsoft Teams 화상 미팅)

참가 인원 : Intentionally deleted

세션 주제 : Security and Cryptography

활동 세부내용

열 번째 세션 주제는 Security and Cryptography입니다. 수업 순서는 Entropy, Hash Function, Key Derivation Function, Symmetric Cryptography, Asymmetric Cryptography 개념 소개로 이루어졌습니다. 보안과 암호학에 관한 내용은 방대하여 하루만에 일련의 작업을 할 수 있을 정도의 수준에 이르기는 힘들기 때문에, 암호학에 사용되는 중요한 개념들과 용어를 비유와 예시를 통해 알기 쉽게 전달하는 것에 초점을 맞추었습니다.

먼저 비밀번호의 강력함을 측정하는 가장 기본적인 단위인 Entropy에 대한 개념을 소개하였습니다. 엔트로피라는 용어는 물리, 화학, 수학에서도 흔히 들어본 개념이기 때문에 용어 자체가 내포하는 의미를 이해시키는 데에는 큰 어려움이 없었습니다. 암호학에서 엔트로피는 발생 가능한 모든 경우의 수에 밑이 2인 로그를 취한 값으로, 동전 던지기의 경우는 1 bit, 주사위 던지기의 경우는 2.58 bits의 엔트로피를 가집니다.

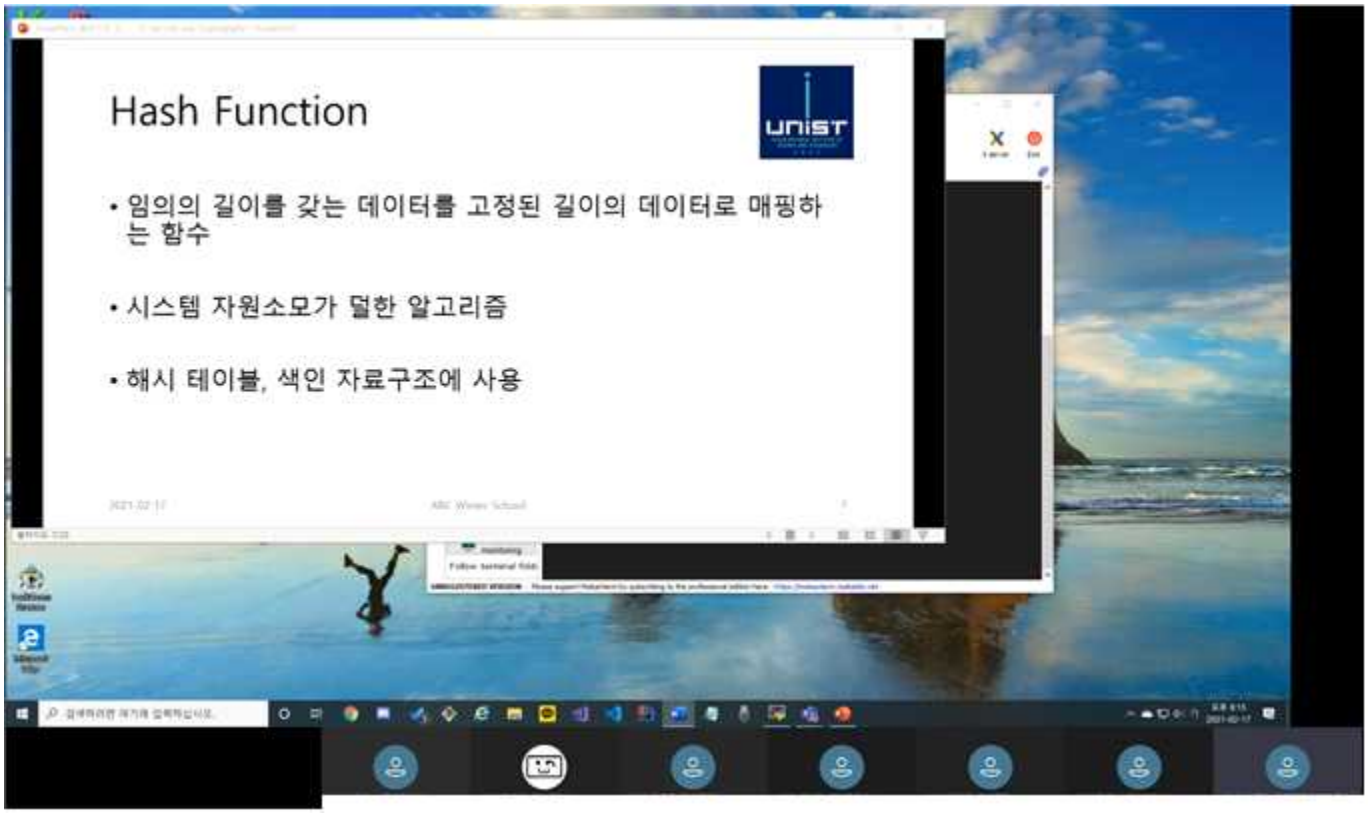
다음 소개한 개념은 해쉬 함수입니다. 해쉬 함수는 임의의 길이를 갖는 데이터를 고정된 길이의 데이터로 매핑해주는 함수입니다. 해쉬 함수는 자료구조론에서 배우는 해쉬 자료구조를 구성하는 중요한 개념이기 때문에, 해쉬 자료구조도 간략히 소개하며 SHA 계열 해쉬함수를 쉘에서 작동시켜보면서 어떤 기능을 하는지 설명하였습니다. 또한, 해쉬 함수는 결정적, 비가역적, 충돌 방어적인 특성을 가지며 Git에서 컨텐츠 보관 주소 생성이나 확약 방식에 사용된다고 설명하였습니다.

Key Derivation Function의 경우는 암호학적 해시 함수와 비슷한 원리로 작동하지만

고의적으로 조금 느리게 설계된 함수입니다. 특히 로그인 신용정보를 저장할 때 사용되는데, 고의적으로 느리게 작동되기 때문에 브루트 포스 기법의 공격을 효과적으로 방어할 수 있습니다.

대칭 암호화와 비대칭 암호화는 개념설명과 더불어 비유를 사용하여 둘의 차이점을 이해할 수 있도록 설명하였습니다. 대칭 암호화는 특정 키로 암호화와 복호화 모두를 수행하게 되지만, 비대칭 암호화는 사설 키와 공용 키 두 가지의 키가 존재하고 각각 복호화와 암호화의 역할을 수행합니다. 대칭 암호화 기법은 파일을 암호화할 때 사용되고 비대칭 암호화 방식은 개인 메신져, Git, 공인 인증 등에서 사용되는 암호화 기법입니다. 대칭 암호화는 귀중품을 보관하고 있는 열쇠 금고에 비유할 수 있는데, 열쇠를 갖고 있다면 귀중품을 꺼내거나 보관할 수 있습니다. 반면, 비대칭 암호화는 자물쇠에 비유할 수 있고 사설 열쇠가 없어도 공개된 공개 키만 갖고 있으면 귀중품을 사물함에 넣고 자물쇠를 채울 수가 있습니다. 하지만 개인 키가 없다면 자물쇠를 열 수 없기 때문에 보관된 귀중품을 꺼낼 수 없습니다. 이처럼 두 가지 방식에는 암호화와 복호화를 할 수 있는 주체에 차이가 있다는 점을 강조하여 설명하였습니다.

활동 사진



슬라이드 노트

Security and Cryptography - 10

A Basic CS skill, ABC winter school

차준형

Department of Computer Science and Engineering

1

Contents

- Entropy
- Hash Function
- Key Derivation Function
- Symmetric Cryptography
- Asymmetric Cryptography

2

Entropy

- '무작위성'의 측정 단위
- 비밀번호가 얼마나 강력한지 척도를 메길 때 유용함

3

Entropy

Tr0ub4dor&3 VS correct horse battery staple

더 강력한 비밀번호는?

4

Entropy

Tr0ub4dor&3 VS correct horse battery staple

- 28bits = 2^28 경우의 수
- 1000번/초 기준 3일 소요
- 해독 쉬움
- 기억하기 어려움

- 44bits = 2^44 경우의 수
- 1000번/초 기준 550년 소요
- 해독 어려움
- 기억하기 쉬움

5

Entropy

- $\log_2$(모든 경우의 수) = Entropy
- Entropy(동전 던지기) = 1
- Entropy(주사위 던지기) = 2.58

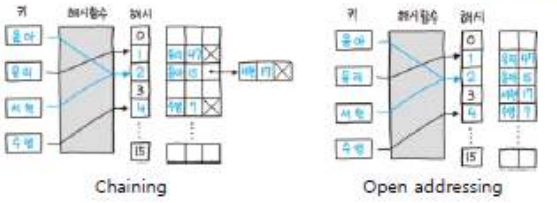
6

Hash Function

- 임의의 길이를 갖는 데이터를 고정된 길이의 데이터로 매핑하는 함수
- 시스템 자원소모가 덜한 알고리즘
- 해시 테이블, 색인 자료구조에 사용

7

Hash Function



8

Hash Function

- 암호학적 해시 함수는 다음과 같은 특성을 가짐
- 1. Deterministic
- 2. Non-invertible
  - hash(message) = h 일 때, h 값으로 messag를 알 수 없다.
- 3. Collision Resistant
  - 서로 다른 input_1과 input_2에 대하여 hash(input_1) != hash(input_2)

9

Hash Function

- SHA 1 : Git에서 커밋 주소를 저장할 때 사용하는 해시 함수.
- 임의의 길이를 가진 입력을 160bit 길이의 데이터로 치환.
  - (40자리의 16진수 수)

10

Hash Function의 사용

- Git의 컨텐츠 주소 저장용으로 사용
- 확약 방식 (Commitment Schemes)

11

Key Derivation Function

- 암호학적 해시 함수와 비슷한 원리로 작동
- 키 복제, 혹은 다른 암호화 알고리즘에 사용될 키로 사용하기 위해 사용함
- KDF는 고의적으로 조금 느리게 설계됨

12

Key Derivation Function의 사용

- 로그인 신용정보를 저장할 때 사용
  - 사용자 마다 salt 값 배정 (salt = random())
  - 비밀번호를 DB에 저장시 KDF(password + salt) 값을 저장
  - 다음 로그인 시, password와 user의 salt값을 조합하여 KDF 함수에 대입
  - KDF(password + salt)값이 존재하면 로그인

13

Symmetric Cryptography

- 대칭 암호화
- 특정 키로 암호화와 복호화를 수행함
- keygen() -> key
- encrypt(plaintext: array<byte>, key) -> array<byte> (the ciphertext)
- decrypt(ciphertext: array<byte>, key) -> array<byte> (the plaintext)

14

Symmetric Cryptography의 사용

- AES
- 클라우드 서비스에 파일 저장할 때 사용

  Key = KDF(password)

  New = Encrpyt(FILE, KEY)

15

Asymmetric Cryptography

- 비대칭 암호화
- public key와 private key를 이용

keygen() -> (public key, private key)

encrypt(plaintext: array<byte>, public key) -> array<byte> (the ciphertext)
decrypt(ciphertext: array<byte>, private key) -> array<byte> (the plaintext)

sign(message: array<byte>, private key) -> array<byte> (the signature)
verify(message: array<byte>, signature: array<byte>, public key) -> bool

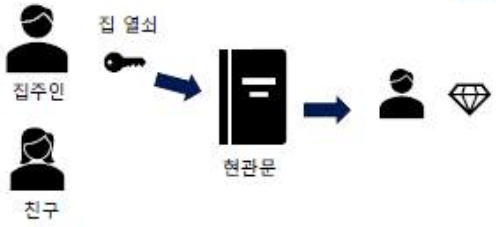
16

Asymmetric Cryptography의 사용

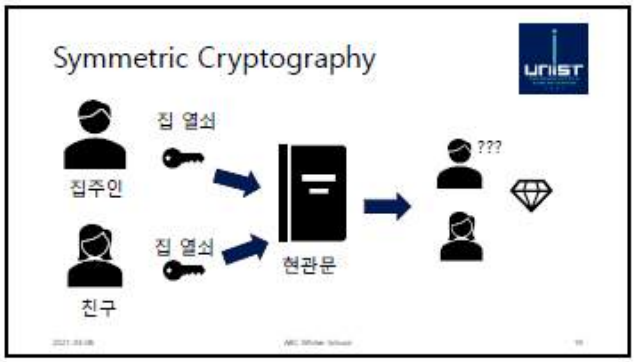
- 개인 메신져 앱 : Telegram, What's App, Signal
- 인증 소프트웨어 : Git, 공인인증 등

17

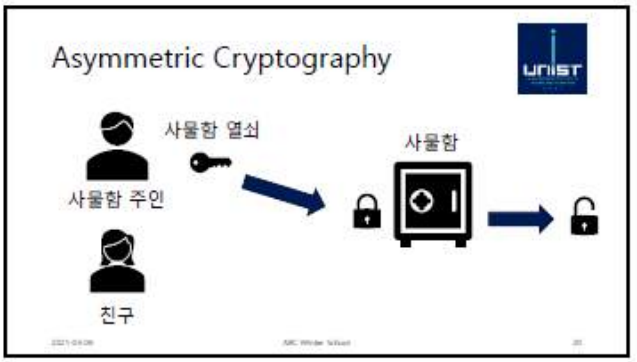
Symmetric Cryptography



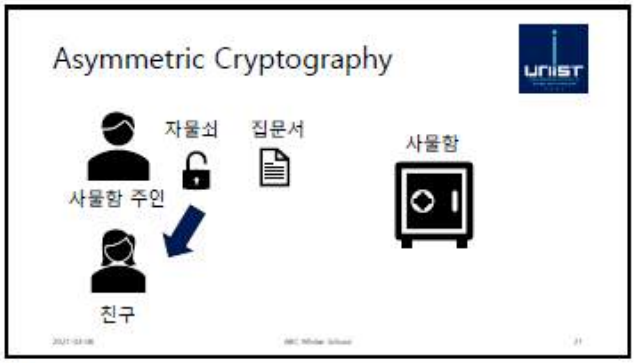
18



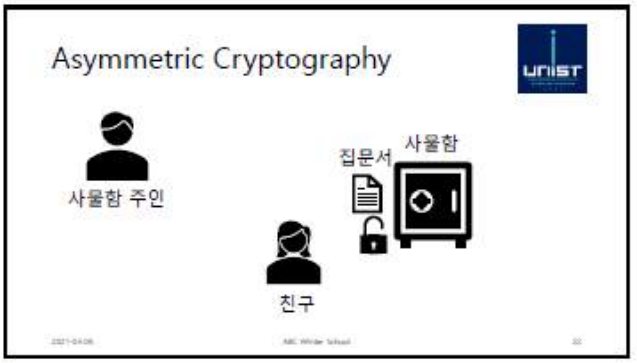
19



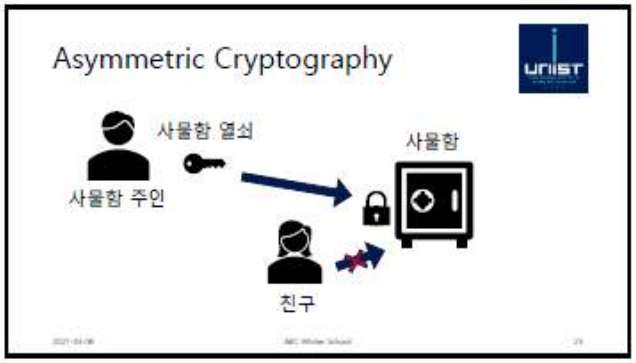
20



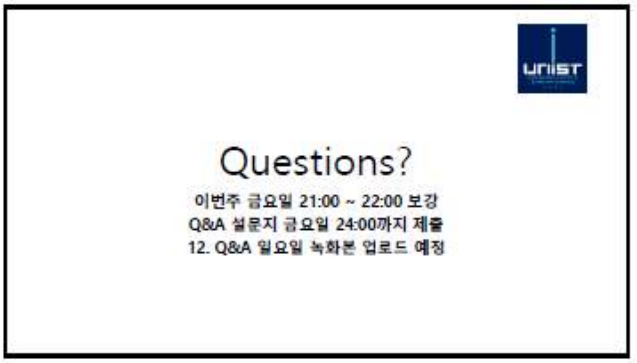
21



22



23



24