Chapter 11
Cryptographic Hash Functions

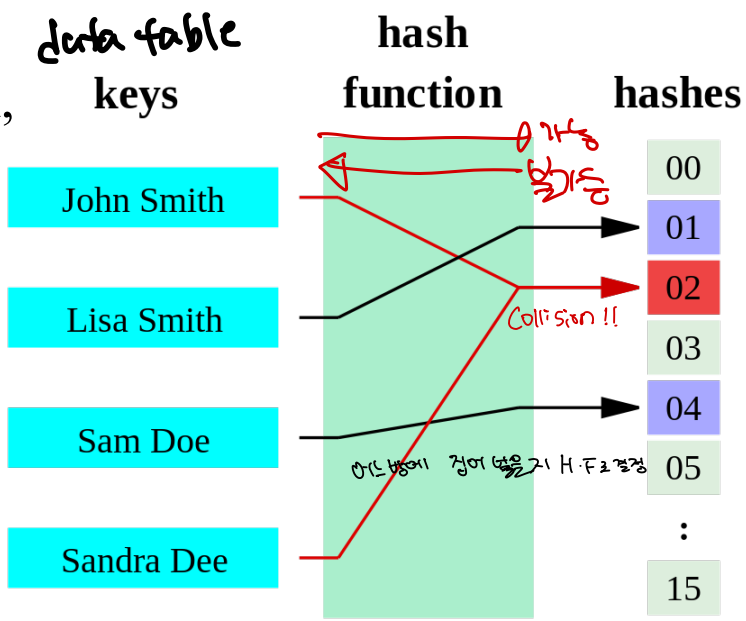
정보보안

Hash Function

- Definition 변수가 없이 암호화 다양한 길이의 입력. 정해진 길이 출력
  - A hash function H(·) is an algorithm that maps data sets of variable length to data sets of a fixed length. The values returned by a hash function are called hash values, hash codes, checksums or simply hashes. In cryptography, the data to be encoded are the message and the hash value is sometimes called the message digest or simply digest.

m가 Hash f 입력

- Example
  - A person's name, having a variable length, could be hashed to a single integer of bounded size.



- Main application
  - Hash tables 어떻게하면 collision 줄일까?

constant time

Cryptographic Hash Function

Key가 없음. 다름

- Pre-image resistance 출력을 알려주고 입력값 찾아봐.
  - Given a hash value h it should be difficult to find any message m such that $h = \mathrm{H}(m)$. $y = H(x)$
- Second pre-image resistance 입력과 출력을 알려줌. 출력에 모는거 하나더 찾아와
  - Given an input m_1 it should be difficult to find another input m_2 such that $m_1 \neq m_2$ and $\mathrm{H}(m_1) = \mathrm{H}(m_2)$. 다른거 하나더 찾아와
  - This property is sometimes referred to as weak collision resistance.
- Collision resistance 출력이 같아지는 x_1, x_2 찾아와. y 안알려줌
  - It should be difficult to find two different messages m_1 and m_2 such that $\mathrm{H}(m_1) = \mathrm{H}(m_2)$. Such a pair is called a cryptographic hash collision.
  - This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for preimage-resistance; otherwise collisions may be found by a birthday attack. 아무런 collision 이나 찾아와

Birthday Attack

- Birthday problem

  계산하고 나면 오류라고 착각

  - In probability theory, the birthday problem or birthday paradox concerns the probability that, in a set of randomly chosen people, some pair of them will have the same birthday.
  - By the pigeonhole principle, the probability reaches 100% when the number of people reaches 366; where we do not consider February 29.
  - The probability reaches 50% with 23 people.

    366명이 있으면 100% collision

    50% 확률로 그냥 생일이 같을려면 23명 필요

- Birthday attack
  - Given a hash function H(·), the goal of the attack is to find a collision. If the hash function yields N different outputs with equal probability, we need to apply H to $\alpha \approx \sqrt{N}$ inputs to have at least one collision with a probability greater than 0.5. For example, $n = 2^{160}$ gives $\alpha \approx 2^{80}$.

n개 input, $\sqrt{n}$ 시도 50% collision

Security Level

- For a hash code of length n, the level of effort required by the opponent is as follows.

Preimage resistant	2^n
Second preimage resistant	2^n
Collision resistant	$2^{n/2}$

256 bit 정도 써주어야 보통

256 개라면 2^{256} 정도 필요

AES-128 이상

보통한다는 것은: 256 bit

- Note that digital signature schemes require the collision resistance.

몇 시쯤 오셨는?

Example: Variations with the same meaning

As {the / —} Dean of Blakewell College, I have {had the pleasure of knowing / known} Cherise Rosetti for the {last / past} four years. She {has been / was} {a tremendous / an outstanding} {asset to / role model in} {our / the} school. I {would like to take this opportunity to / wholeheartedly} recommend Cherise for your {school's / —} graduate program. I {am / feel} {confident / certain} {that / —} {she / Cherise} will {continue to / —} succeed in her studies. {She / Cherise} is a dedicated student and {thus far her grades / her grades thus far} {have been / are} {exemplary / excellent}. In class, {she / Cherise} {has proven to be / has been} a take-charge {person / individual} {who is / —} able to successfully develop plans and implement them.

{She / Cherise} has also assisted {us / —} in our admissions office. {She / Cherise} has {successfully / —} demonstrated leadership ability by counseling new and prospective students. {Her / Cherise's} advice has been {a great / of considerable} help to these students, many of whom have {taken time to share / shared} their comments with me regarding her pleasant and {encouraging / reassuring} attitude. {For these reasons / It is for these reasons that} I {highly recommend / offer high recommendations for} Cherise {without reservation / unreservedly}. Her {ambition / drive} and {abilities / potential} will {truly / surely} be an {asset to / plus for} your {establishment / school}.

General Structure of Hash Function

- The hash algorithm involves repeated use of a compression function, f, that takes two inputs (an n-bit input from the previous step, called the chaining variable, and a b-bit block) and produces an n-bit output.

$$CV_0 = IV = \text{initial n-bit value}$$

$$CV_i = f(CV_{i-1}, Y_{i-1}) \quad \text{where } 1 \leq i \leq L$$

$$H(M) = CV_L$$

where the input to the hash function is a message M consisting of the blocks $Y_0, Y_1, \ldots, Y_{L-1}$.

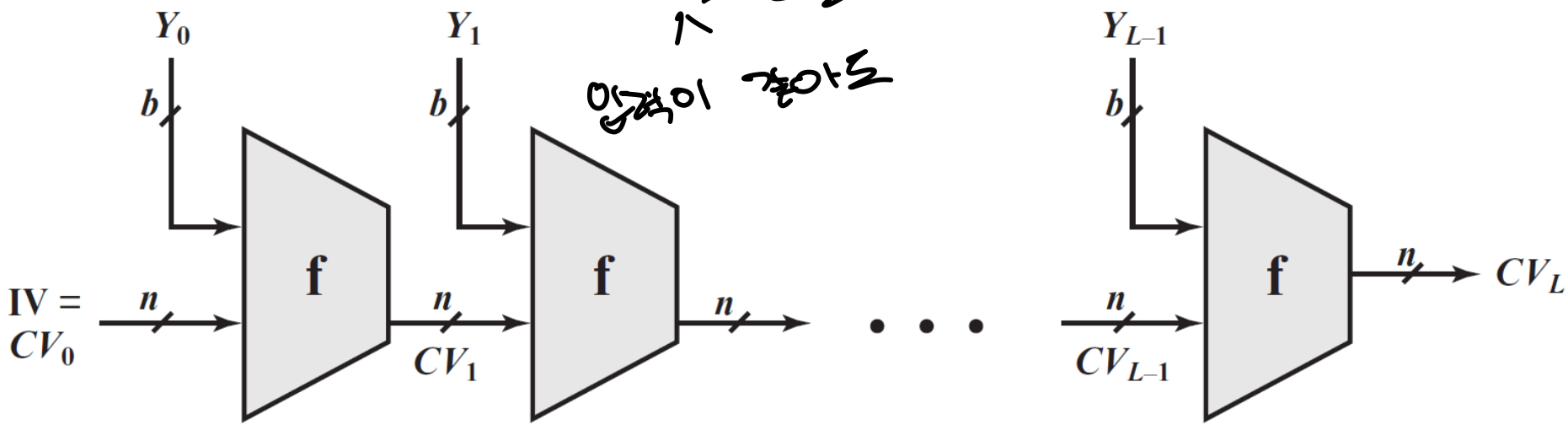
General Structure of Hash Function

T = 메시지

deterministic 함. 메시지 숨기는 목적 X

매번 출력이 다르게 나올 필요 X

암호학이 좋아도



IV = Initial value
CV_i = Chaining variable
Y_i = ith input block
f = Compression algorithm
L = Number of input blocks
n = Length of hash code
b = Length of input block

복구 X 단 특징인데, 지문값. 지문으로부터 사람데이터 복구 X

사람을 대신해서 지문값 사용

Cryptographic Hash Functions in Practice

- MD5
  - 128-bit output. 고정
  - MD5 was introduced in 1991… collision attacks found in 2004… several extensions and improvements since then.
  - However, MD5 is still widely deployed(!)
- SHA (Secure Hash Algorithm)
  - The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).

SHA (Secure Hash Algorithm)

- SHA-0
  - A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA." It was withdrawn shortly after publication due to an undisclosed significant flaw and replaced by the slightly revised version SHA-1.
- SHA-1
  - A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the NSA to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.
- SHA-2
  - A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. There are also truncated versions of each standardized, known as SHA-224 and SHA-384.
- SHA-3
  - A hash function formerly called Keccak, chosen in 2012 after a public competition. It supports variable output length (224, 256, 384, 512), and its internal structure differs significantly from the rest of the SHA family.

SHA-1/SHA-2 Parameters

Algorithm	Message Size	Block Size	Word Size	Message Digest Size
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

(All sizes are measured in bits.)

SHA-3 Parameters

Message Digest Size	224	256	384	512
Message Size	no maximum	no maximum	no maximum	no maximum
Block Size (bitrate *r*)	1152	1088	832	576
Word Size	64	64	64	64
Number of Rounds	24	24	24	24
Capacity *c*	448	512	768	1024
Collision Resistance	2^{112}	2^{128}	2^{192}	2^{256}
Second Preimage Resistance	2^{224}	2^{256}	2^{384}	2^{512}

메시지 사이즈 한계 X

Birthday 때문에 안전도는 절반.

Cryptographic Hash Functions: Applications

- Motivation
  - Cryptographic hash values are sometimes called (digital) fingerprints.
- Applications
  - Verifying the integrity of files or messages
  - Password files

File Hash Checking

Downloads

Here you find the current installation package of MAMP & MAMP PRO.

Mac OS X | **Windows**

MAMP & MAMP PRO 3.3.0 (Windows)

Download

SHA-256: adbfc53a3aa5a02f3a00f7c96b61f4b1704e2811e757db223eea658d705b039c

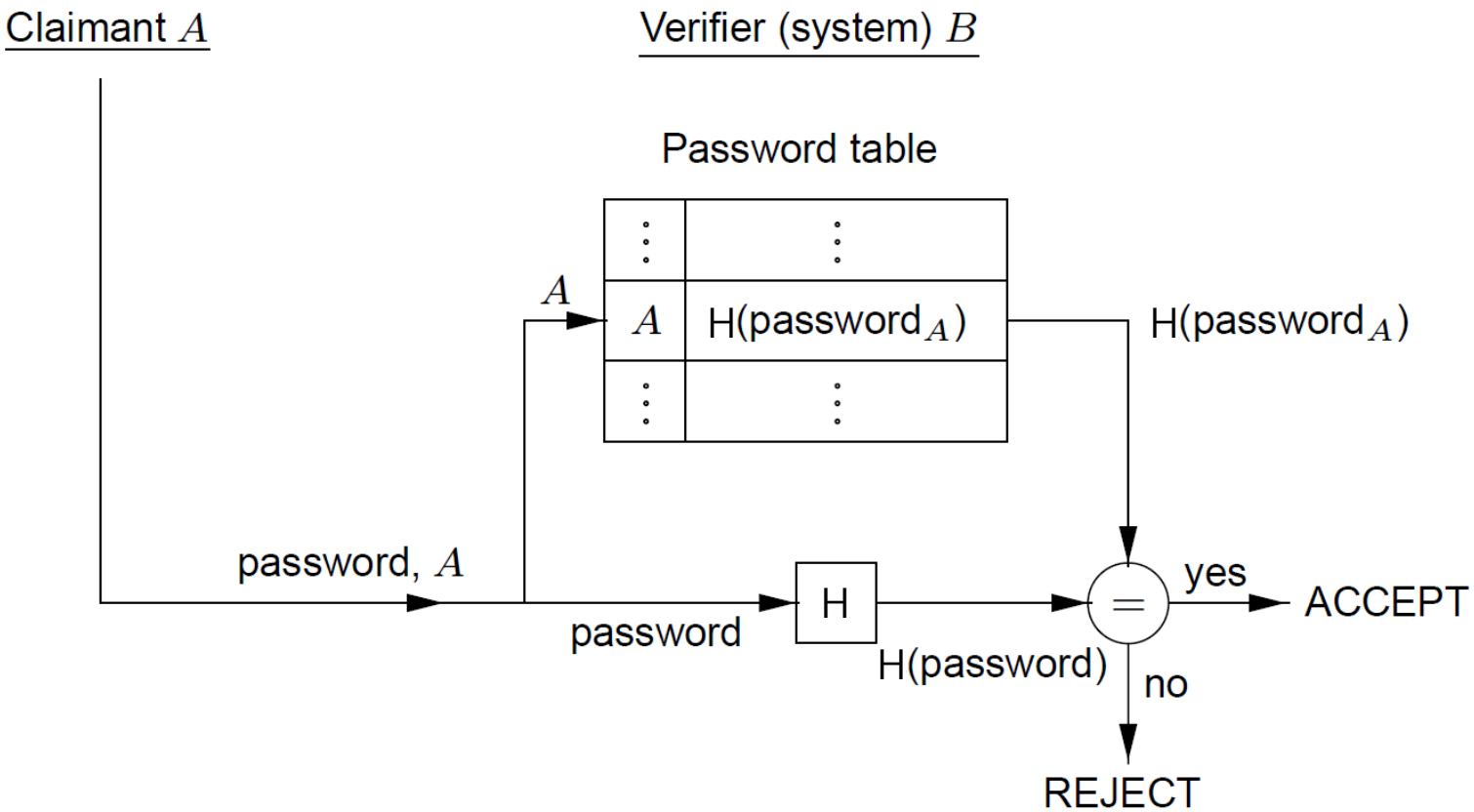
This download package for Windows contains the free MAMP and a free 14-day trial of MAMP PRO. MAMP can be used stand-alone without MAMP PRO.

The trial Version of MAMP PRO can be upgraded to the full version by buying a serial number.

Components

Apache: 2.2.31
Nginx 1.11.0
MySQL: 5.6.34
PHP: 5.3.23 & 5.4.1 & 5.4.45 & 5.5.0 & 5.5.24 & 5.5.38 & 5.6.0 & 5.6.28 & 7.0.0 & 7.0.6 & 7.0.13 (for PHP 7: Windows 7 minimum with SP1 and Windows

Password Hashing



Salting passwords

– To make dictionary attacks less effective, each password may be augmented with a t-bit random string called a salt before applying H.