Session 05

Hash Functions

CS 7349

Spring 2024

World Changers Shaped Here

SMU

Contents

- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Quick review
- Hash Functions

Sources: YouTube/Dr. Dan Boneh, Cryptography 1; Cryptography and Network Security, William Stallings;

House Keeping

- Status of Teams for Term Paper? Topic?
- Research Paper submit Jan deliverables now;
- Checkpoint on 02/15, 02/19
- Submit Quiz 2 and start on Quiz 3; Case Study published
- Submit HW1 and start Case Study
- Quiz 2, 1 week; Case Study, 2 weeks
- RED ALERT on Research Paper! Teams & Topic NOW!!

CS7349 Slay status next week?

Sources: Meta AI

Security News of the Week – Spring 2024

- https://www.wired.com/story/27-year-old-codebreaker-busted-myth-bitcoins-anonymity/#intcid=_wired-tag-right-rail_5368081e-380a-4ef5-adc6-53949cb77cb3_popular4-1
  - Book Review: How a grad student derailed bitcoin anonymity
- https://www.securityweek.com/schneider-electric-division-responding-to-ransomware-attack-data-breach/
  - Schneider Electric division reported a ransomware attack started ~01/17
- https://www.wsj.com/articles/intelligence-researchers-to-study-computer-code-for-clues-to-hackers-identities-e1d594a4?mod=cybersecurity_more_article_pos1
  - Research: How to find hacker identity?

Source: wsj.com; securityweek.com;wired.com

DS 7349 – Tying it all together

Confidentiality	Integrity Availability	Networks/Application
INTRODUCTION TO DS7349 AND THE THREAT LANDSCAPE	HASH FUNCTIONS	NETWORK SECURITY
INTRODUCTION TO NETWORKS	MESSAGE AUTHENTICATION CODES	SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
SYMMETRIC KEY CRYPTO	KEY MANAGEMENT	FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
USING SYMMETRIC KEY CIPHERS	IDENTITY AND ACCESS MANAGEMENT	REVIEW/ADDITIONAL TOPICS
RANDOMNESS AND PSEUDORANDOM NUMBERS		
PUBLIC KEY CRYPTO/Team Paper		

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, ~~Braden~~, ~~Cho~~, Dominguez, Garcia, Garza, Gibbs, Guo, Hennes, Jackson, Kharwadhkar, Kucera, Lei, Liang, Lim, Lin, Liu, Magee, Mandalaneni, Mathew, Miller, Nagamanickam, DPatel, PPatel, Pittman, Sanaboyina, Singh, Skochdopole, Swigart, Taghavi, Wang, Werth, Zhai

Project Timeline (For 9 page paper)

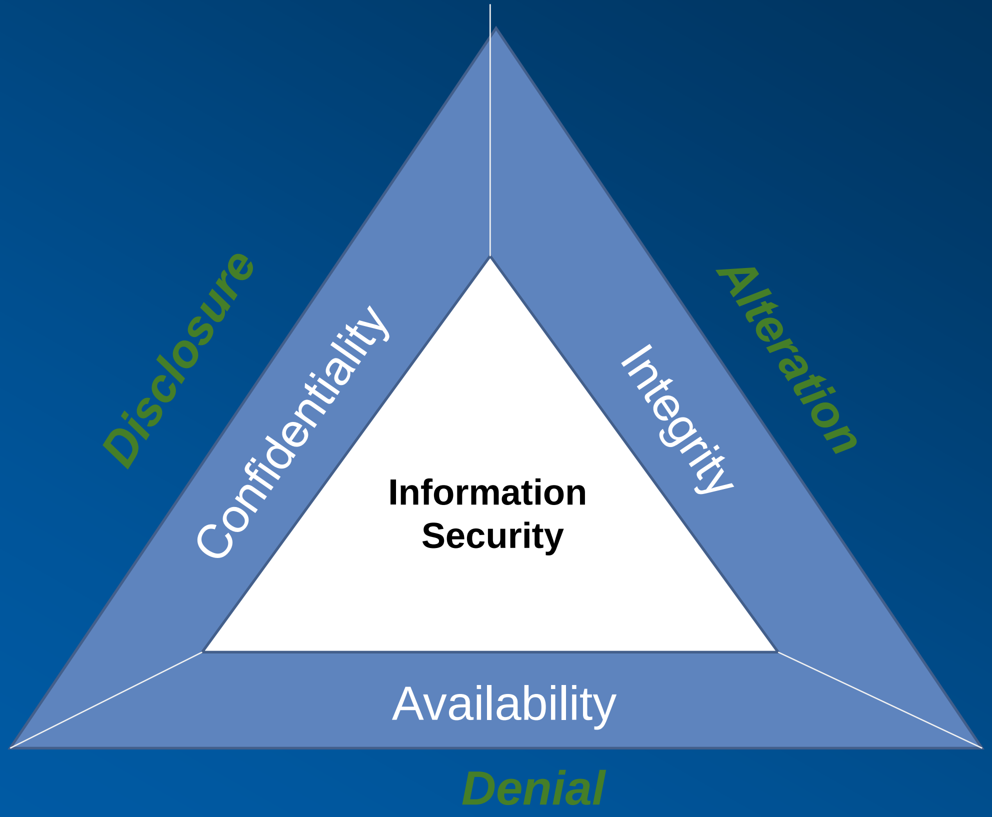
- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

Project – 1st deliverable

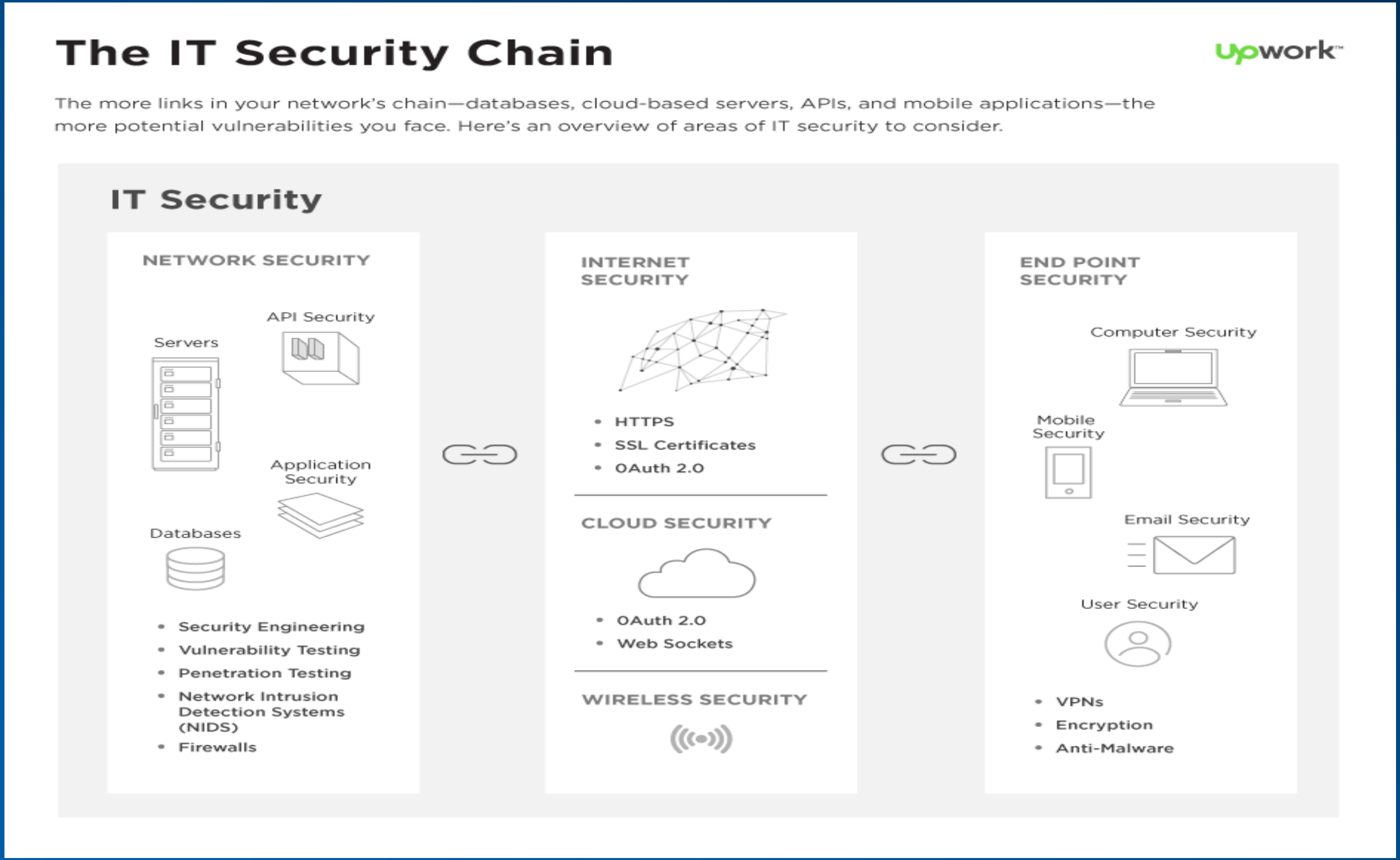
- Team projects (3 per team)
- Choose topic (from topic list or your own)*
- Within topic, identify problem to be addressed (no survey projects, only problem solving projects - survey is a part of your problem solution and is contained in the final paper)
- Confirm problem with professor

InfoSec, CIA, Threats



Source: "Information Security Illuminated", Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics



Source: Upwork Global, Inc

Hash Functions

- A hash function H accepts a variable-length block of data *M* as input and produces a fixed-size hash value
  - $h = \mathrm{H}(M)$
  - Principal objective is data integrity
- Cryptographic hash function
  - An algorithm for which it is computationally infeasible to find either:

    (a) a data object that maps to a pre-specified hash result (the one-way property)

    (b) two data objects that map to the same hash result (the collision-free property)

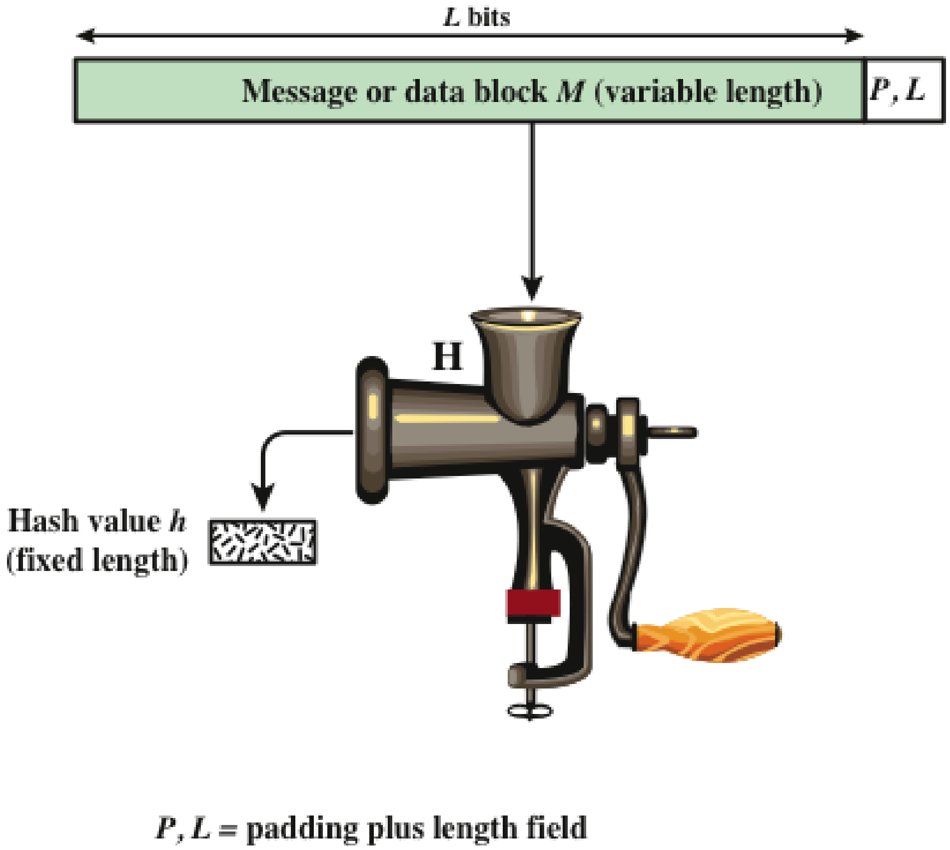
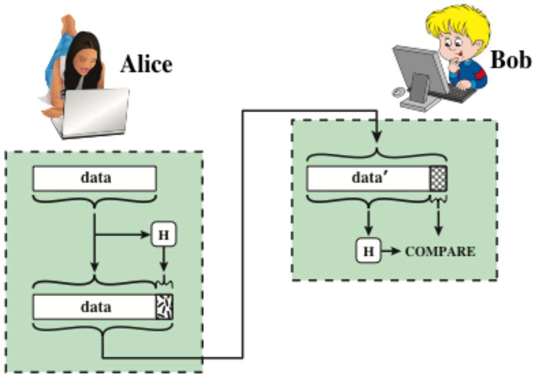
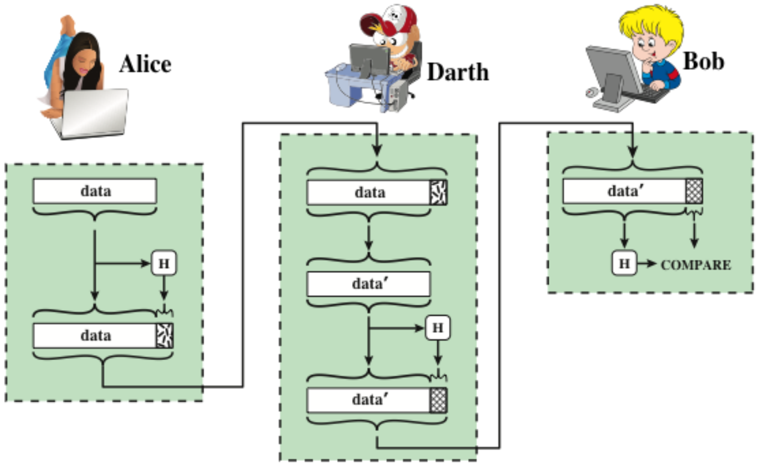


Figure 11.1 Cryptographic Hash Function; $h = \mathrm{H}(M)$



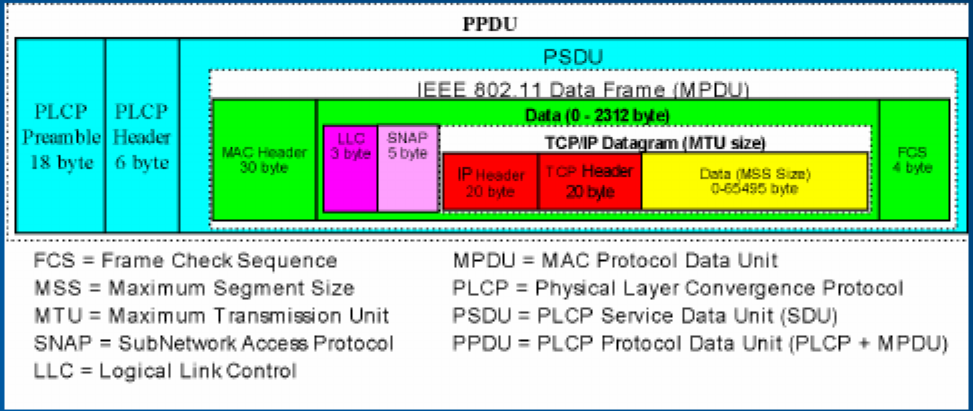
(a) Use of hash function to check data integrity



(b) Man-in-the-middle attack

Figure 11.2 Attack Against Hash Function

Message Authentication Code (MAC)



- Also known as a *keyed hash function*
- Typically used between two parties that share a secret key to authenticate information exchanged between those parties

Takes as input a secret key and a data block and produces a hash value (MAC) which is associated with the protected message

- If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value
- An attacker who alters the message will be unable to alter the associated MAC value without knowledge of the secret key

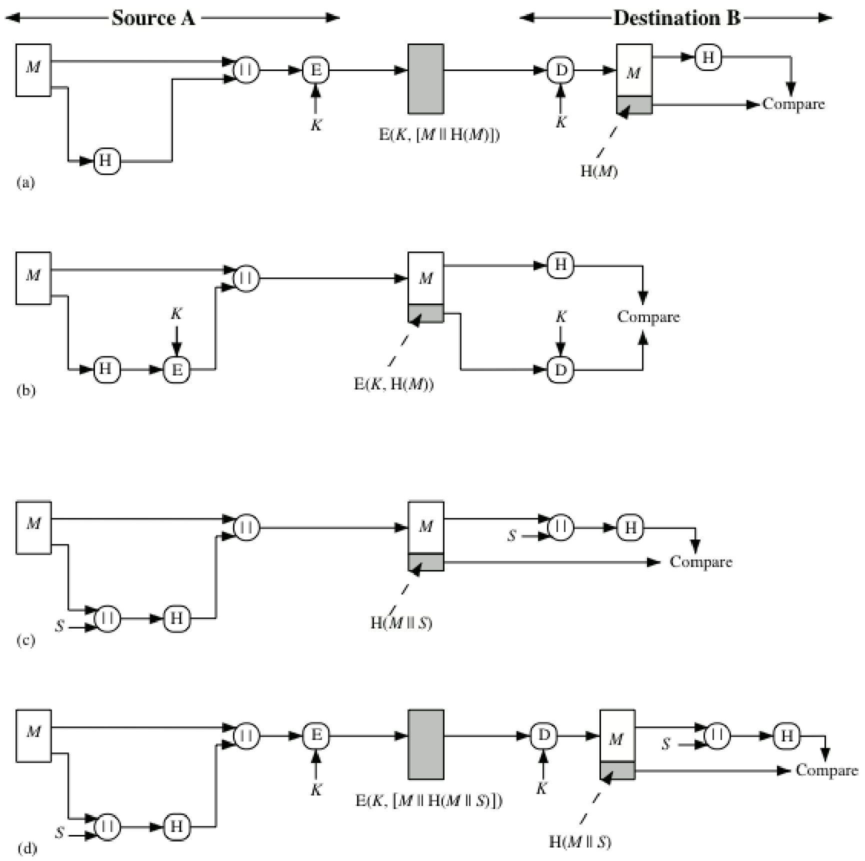


Figure 11.3 Simplified Examples of the Use of a Hash Function for Message Authentication

$E_{(M+H)}$, Symmetric

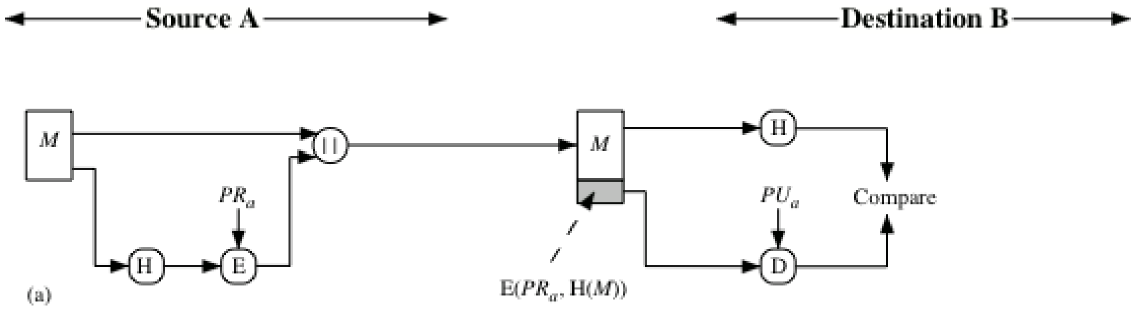
H_E, Symmetric

M+H, s, Sign/Verify

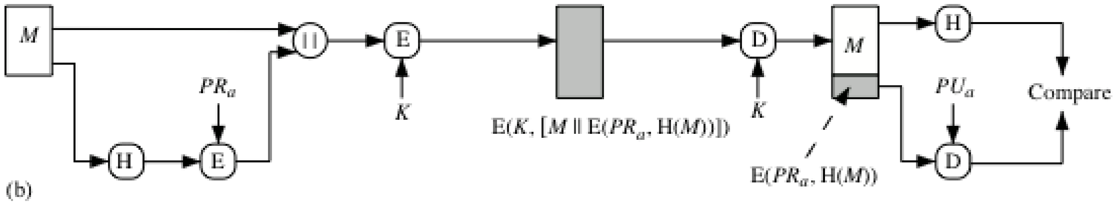
E(M+H), s, Sign/Verify

Digital Signature

- Operation is similar to that of the MAC
- The message hash value is encrypted with a user's private key
- User's public key can verify the integrity of the message
- To alter the message would need to know the user's private key
- Implications of digital signatures go beyond just message authentication



Authentication, Digital Signature



Authentication, Digital Signature, Confidentiality

Figure 11.4 Simplified Examples of Digital Signatures

Other Hash Function Uses

Commonly used to create a one-way password file

- When a user enters a password, the hash of that password is compared to the stored hash value for verification
- This approach to password protection is used by most operating systems

Can be used for intrusion and virus detection

- Store H(F) for each file on a system and secure the hash values
- One can later determine if a file has been modified by recomputing H(F)
- An intruder would need to change F without changing H(F)

Can be used to construct a pseudorandom function (PRF) or a pseudorandom number generator (PRNG)

- A common application for a hash-based PRF is for the generation of symmetric keys

Requirements and Security

Preimage

- x is the preimage of h for a hash value $h = H(x)$
- Is a data block whose hash function, using the function H, is h
- Because H is a many-to-one mapping, for any given hash value h, there will in general be multiple preimages

Collision

- Occurs if we have $x \neq y$ and $H(x) = H(y)$
- Because we are using hash functions for data integrity, collisions are clearly undesirable

Requirements for Crypto Hash Functions

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
Pseudorandomness	Output of H meets standard tests for pseudorandomness

Attacks on Hash Functions

Brute-Force Attacks

- Not algorithm specific, depends only on bit length
- For a hash function, attack depends only on the bit length of the hash value
- Method is to pick values at random and try each one until a collision occurs

Cryptanalysis

- An attack based on weaknesses in a particular cryptographic algorithm
- Seek to exploit some property of the algorithm to perform some attack other than an exhaustive search

Birthday Attacks

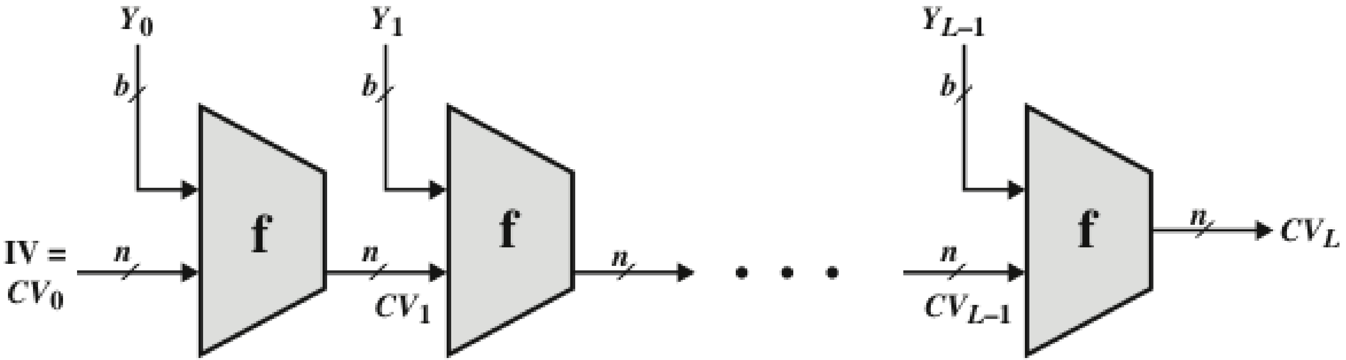
- For a collision resistant attack, an adversary wishes to find two messages or data blocks that yield the same hash function
  - The effort required is explained by a mathematical result known as the *birthday paradox*
- How the birthday attack works:
  - Alice signs a message ***x*** by appending the appropriate *m*-bit hash code and encrypting that hash code with her private key
  - Trudy generates $2^{m/2}$ variations ***x'*** of ***x***, all with essentially the same meaning, and stores the messages and their hash values
  - Trudy generates a fake message *y* for which Alice's signature is needed
  - Two sets of messages are compared to find a pair with the same hash
  - Trudy gives the message to Alice for signature which can then be attached to the fake version to the intended recipient Bob
    - two variations have the same hash code, they will produce the same signature and the opponent is assured of success even though the encryption key is not known

Hash Functions

- Burning questions?

- The math proof behind the birthday paradox
  https://youtu.be/Y_shcEgdhI8

- The Merkle-Damgard Construct for hash functions
  - https://www.youtube.com/watch?v=VCOinPlsThw (start 0:48 – 4:46)



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

Figure 11.8 General Structure of Secure Hash Code

Hash Functions Based on Block Ciphers

Cipher Block Chaining (CBC mode)

- Can use block ciphers as hash functions
  - Using H_0=0 and zero-pad of final block
  - Compute: $H_i = E(M_i\ H_{i-1})$
  - Use final block as the hash value
  - Similar to CBC but without a key

- Resulting hash is too small (64-bit)
  - Both due to direct birthday attack
  - And “meet-in-the-middle” attack

- Other variants also susceptible to attack

Secure Hash Algorithm (SHA)

- SHA was originally designed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993
- Was revised in 1995 as SHA-1
- Based on the hash function MD4. Design closely models MD4
- Produces 160-bit hash values
- In 2002 NIST produced a revised version of the standard that defined three new versions of SHA with hash value lengths of 256, 384, and 512
  - Collectively known as SHA-2

Comparison of SHA Parameters

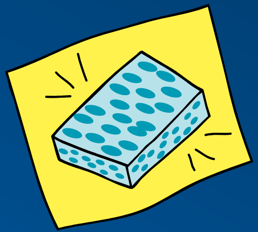
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Note: All sizes are measured in bits.

The Sponge Construction

- Underlying structure of SHA-3 is a scheme referred to by its designers as a *sponge construction*
- Takes an input message and partitions it into fixed-size blocks
- Each block is processed in turn with the output of each iteration fed into the next iteration, finally producing an output block
- The sponge function is defined by three parameters:
  - f = the internal function used to process each input block
  - r = the size in bits of the input blocks, called the *bitrate*
  - pad = the padding algorithm



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}

Thank You!

World Changers
Shaped Here

SMU®

Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (125-150 word limit for 9 pages)
  - start with statement of what is presented (2 sentences)
  - motivate the problem (2-3 sentences)
  - discuss details of what is done at a high level (1-2 sentences)
  - state the main conclusions (1-2 sentences)
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper (2nd last paragraph)
  - state the outline for the rest of the paper (final paragraph)
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template