NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Basic Networking Security

Cloud Infrastructure Engineering

Nanyang Technological University & Skills Union - 2022/2023

Course Content

- Quick Check-In
- Dive into the basics of Network Security
- Explore the importance of Network Security
- Differentiate between Encoding, Hashing, Encryption, and the usage of each
- Come up with solutions to prevent possible security breaches

Time	What	How or Why
7:10pm - 7:20pm	Part 1 - Presentation	Importance of Networking Security
7:20pm - 7:50pm	Part 2 - Presentation	Encoding, Hashing, Encryption & Activities
7:50pm - 8:00pm	Break	
8:00pm - 8:20pm	Part 3 - Presentation	Common Network Security Vulnerabilities & Cyberattacks
8:20pm - 8:40pm	Part 4 - Presentation	Case Studies
8:40pm - 8:45pm	Break	
8:45pm - 8:50pm	Group Assignment Briefing	
8:50pm - 9:20pm	Learners self attempt on group assignments	
9:20pm - 9:40pm	Learners share group assignments	
9:40pm - 10:00pm	Wrap Up	

Recap

- Network Communication Protocol
  - TCP
  - UDP
  - HTTP
  - FTP
- Network Management Protocol
  - ICMP
  - SNMP
- Network Security Protocol
  - HTTPS
  - SSL/ TLS
  - SFTP

Self Study Check-In

Q1) _____ is a reversible transformation of data format, used to preserve usability of data. What does this statement describe?

A) Encoding
B) Hashing
C) Encryption

Q2) _____ is a one-way summary of data, cannot be reversed, used to validate the integrity of data. What does this statement describe?

A) Encoding
B) Hashing
C) Encryption

Q3) _____ is a secure encoding of data used to protect confidentiality of data. What does this statement describe?

A) Encoding
B) Hashing
C) Encryption

Importance of Security

What is Network Security?

Network security consists of all the technologies and practices that **keep computer systems and electronic data safe**.

In a world where more and more of our business and social lives are online, it's **an enormous and growing field with many types of job roles.**

What is Network Security?

According to the Cyber Security & Infrastructure Security Agency (CISA), "Cyber security is the ***art*** of **protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information.**"

Why is Network Security important?

- Protects Your Data
- Protects Client Data
- Prevents Identity Theft

What can Network Security encompass?

Network security

Protects computer networks like home Wi-Fi or a business's network from threats

What can Network Security encompass?

Application security

Ensures programs and apps repel hackers and keep users' data private

What can Network Security encompass?

Cloud security

Focuses on the cloud, where users and businesses store data and run apps online using remote data centers

What can Network Security encompass?

Endpoint security

Practice of **securing endpoints or entry points** of end-user devices such as desktops, laptops, and mobile devices **from being exploited by malicious actors and campaigns.**

Network Security Summary

NAICE

Network security

Application security

Information security

Cloud security

Endpoint security

Encoding, Hashing and Encryption

Encoding

Encoding data is a **process of changing data into another string**.

Encoding is a **reversible process**; meaning that data can be encoded to a new format and decoded to its original format.

Encoding data is typically used to **ensure integrity and usability of data** and is commonly used when data cannot be transferred in its current format between systems or applications.

Encoding is **NOT used to protect or secure data** because it is easy to reverse.

Encoding

A very popular example is base64:

> The base64 is a **binary to a text encoding scheme** that represents binary data in an ASCII string format. **base64 is designed to carry data stored in binary format across the channels**. It takes any form of data and transforms it into a long string of plain text.

GUI - https://www.base64decode.org/

Command Line - https://www.serverlab.ca/tutorials/linux/administration-linux/how-to-base64-encode-and-decode-from-command-line/

Encoding

```
luqmannurhakimbintajuddin@Luqmans-MacBook-Pro ~ % echo -n "Hi I'm Luqman" | base64
SGkgSSdtIEx1cW1hbg==
luqmannurhakimbintajuddin@Luqmans-MacBook-Pro ~ %
```

```
luqmannurhakimbintajuddin@Luqmans-MacBook-Pro ~ % echo -n "SGkgSSdtIEx1cW1hbg==" | base64 --decode
Hi I'm Luqman
luqmannurhakimbintajuddin@Luqmans-MacBook-Pro ~ %
```

Activity Time

In this activity, **decode this message via both browser and command line:**

V2UgYXJlIGxlYXJuaW5nIGFib3V0IFNFQ1VSSVRZIG9uIFNraWxsc1VuaW9uIHRvZGF5LiBBcmUgeW91IGV4aXRlZD8=

Hashing

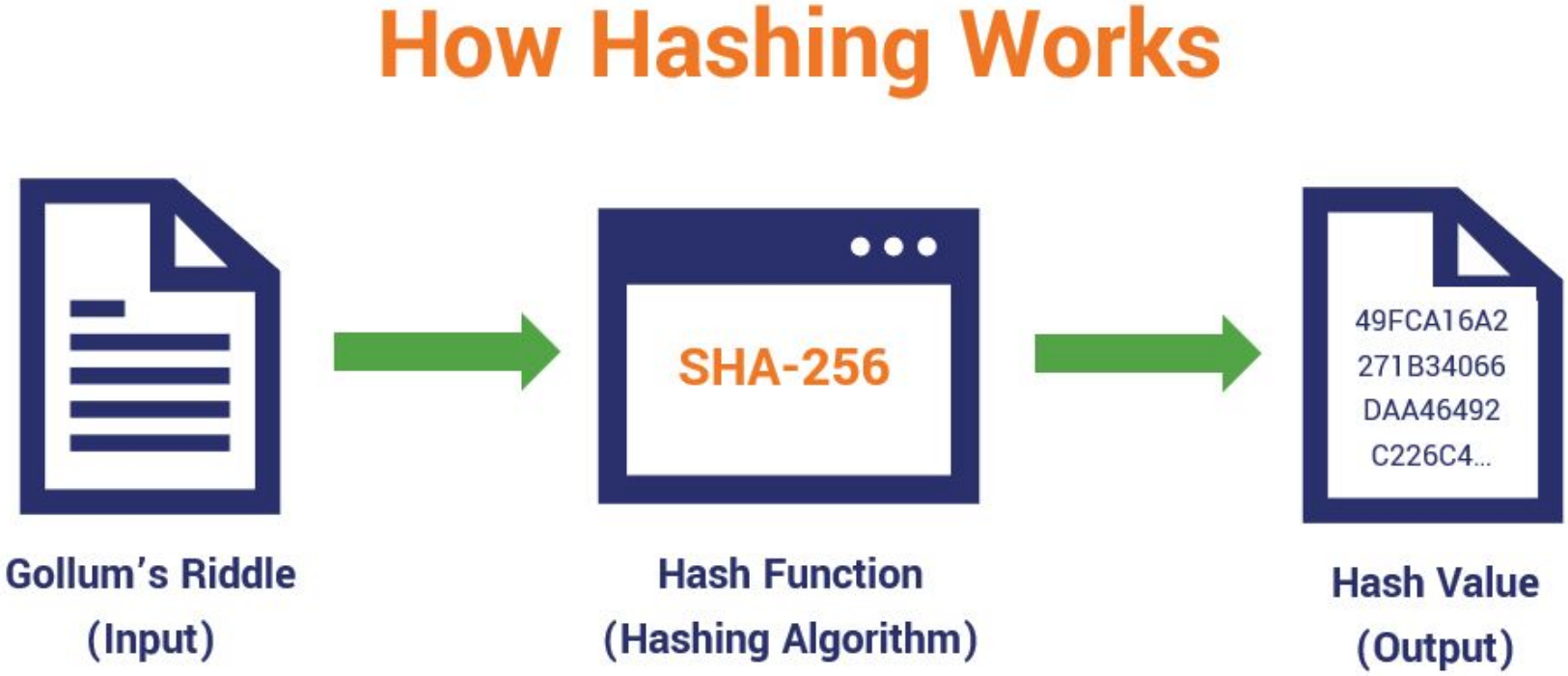
Hashing involves **computing a fixed-length mathematical summary of data**, hence, the input data can be any size.

In contrast to encoding, hashing **cannot be reversed**. It is not possible to take a hash and convert it back to the original data.

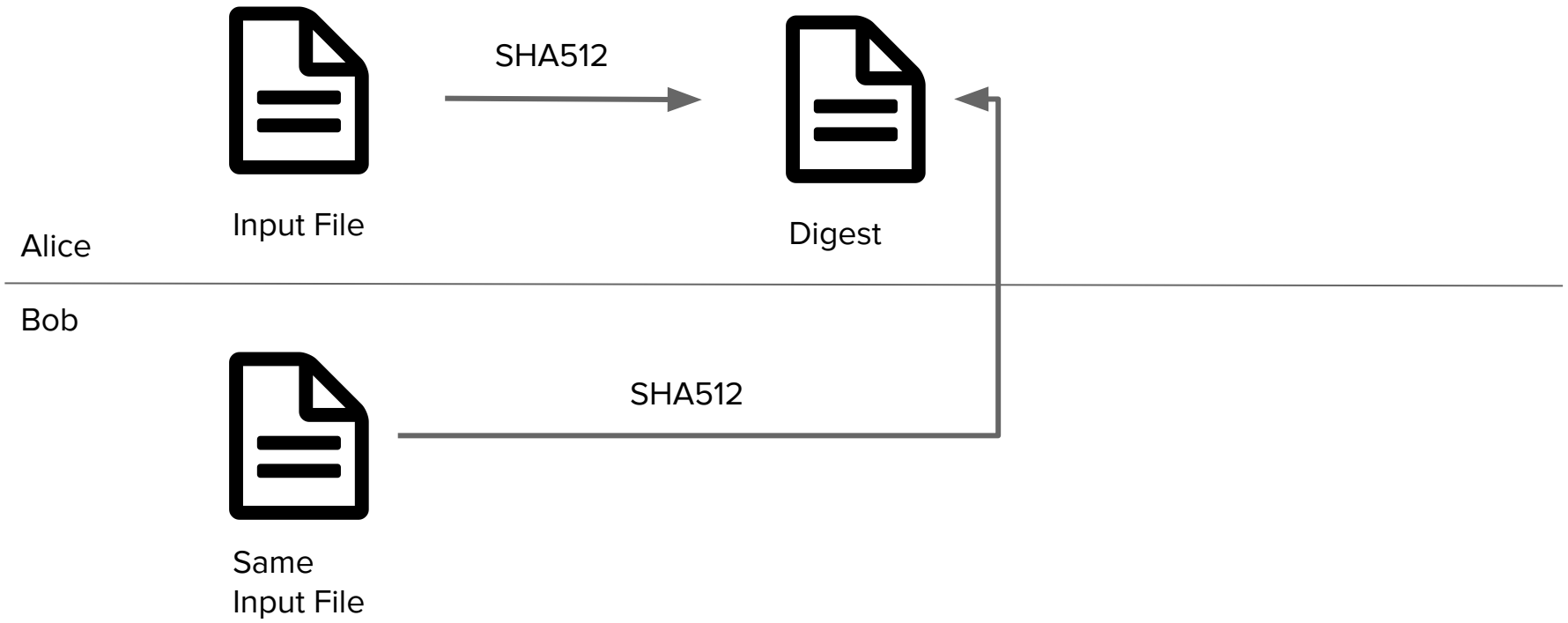
Hashing is commonly used to **verify the integrity of data**, commonly referred to as a checksum.

If two pieces of identical data are hashed using the same hash function, the resulting hash will be identical. If the two pieces of data are different, the resulting hashes will be different and unique.

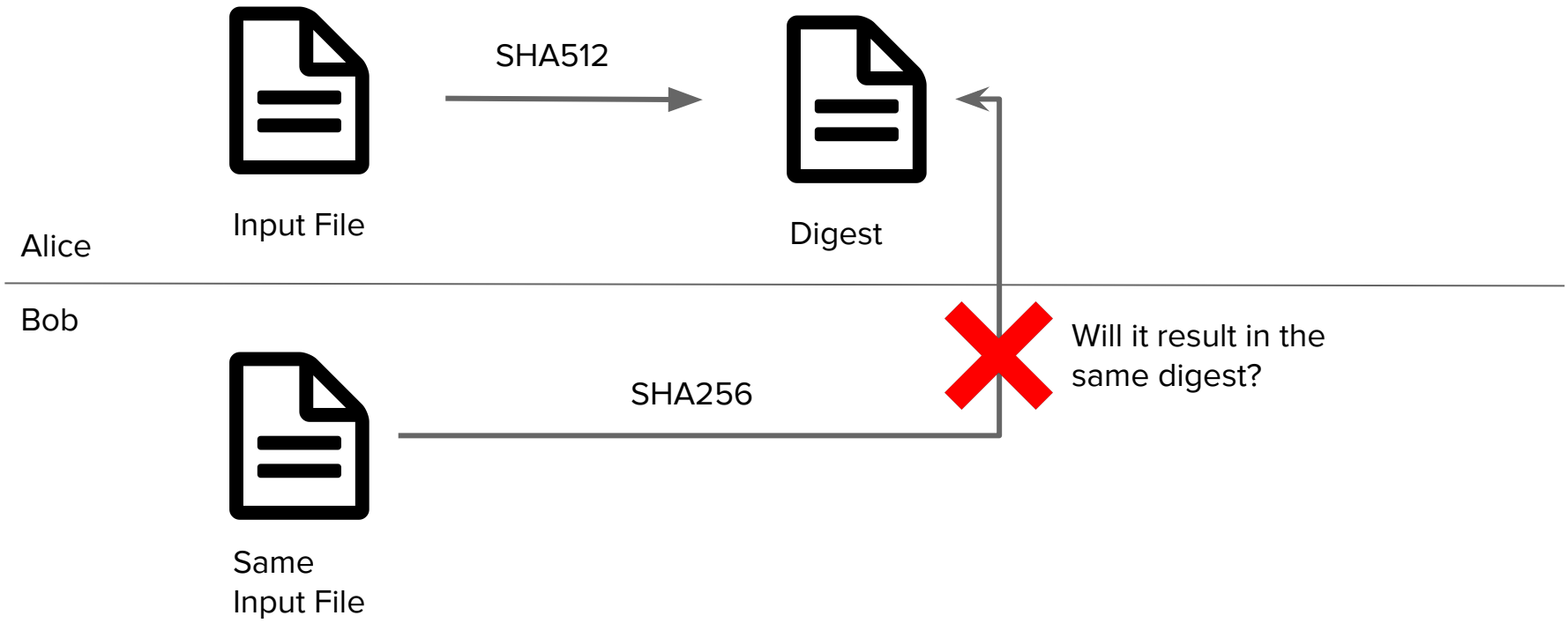
Hashing


How Hashing Works
SHA-256
49FCA16A2
271B34066
DAA46492
C226C4...
Gollum's Riddle
(Input)
Hash Function
(Hashing Algorithm)
Hash Value
(Output)

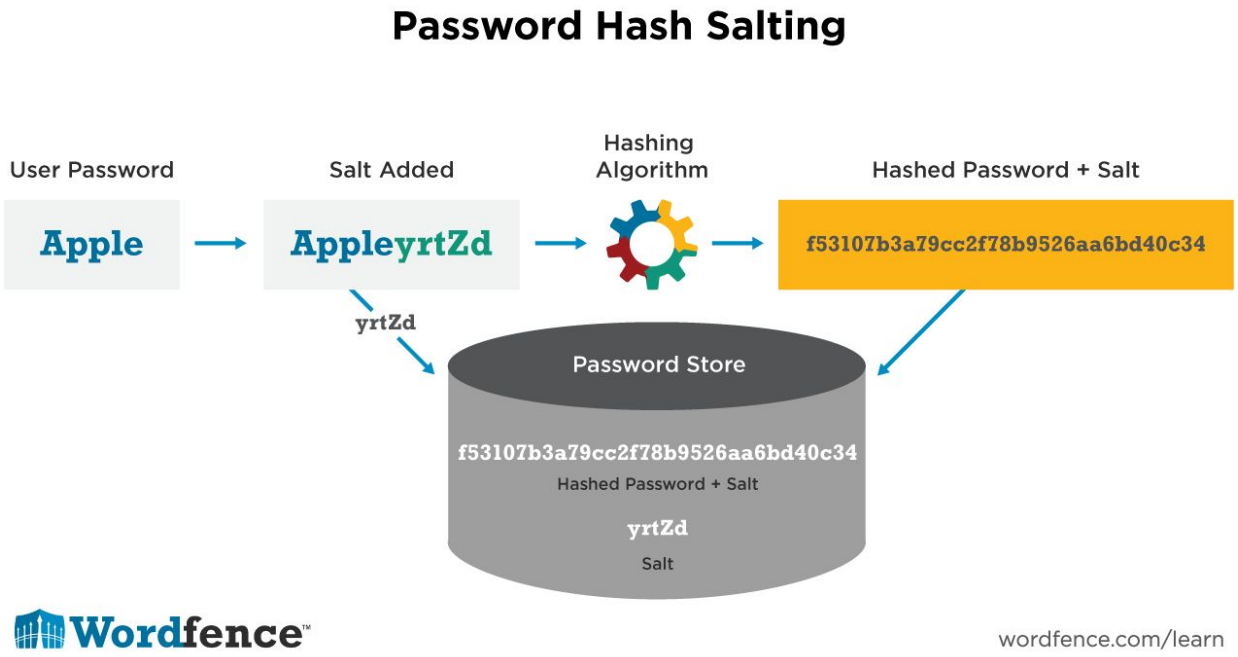
Hashing



Hashing


SHA512
Input File
Digest
Alice
Bob
Will it result in the same digest?
SHA256
Same Input File

Hashing


Password Hash Salting
User Password
Salt Added
Hashing Algorithm
Hashed Password + Salt
Apple
AppleyrtZd
f53107b3a79cc2f78b9526aa6bd40c34
yrtZd
Password Store
f53107b3a79cc2f78b9526aa6bd40c34
Hashed Password + Salt
yrtZd
Salt
Wordfence
wordfence.com/learn

Activity Time

In this activity, **can you guess what is the text resulting in the below SHA512 digest?**

d9e6762dd1c8eaf6d61b3c6192fc408d4d6d5f1176d0c29169bc24e71c3f274a d27fcd5811b313d681f7e55ec02d73d499c95455b6b5bb503acf574fba8ffe85

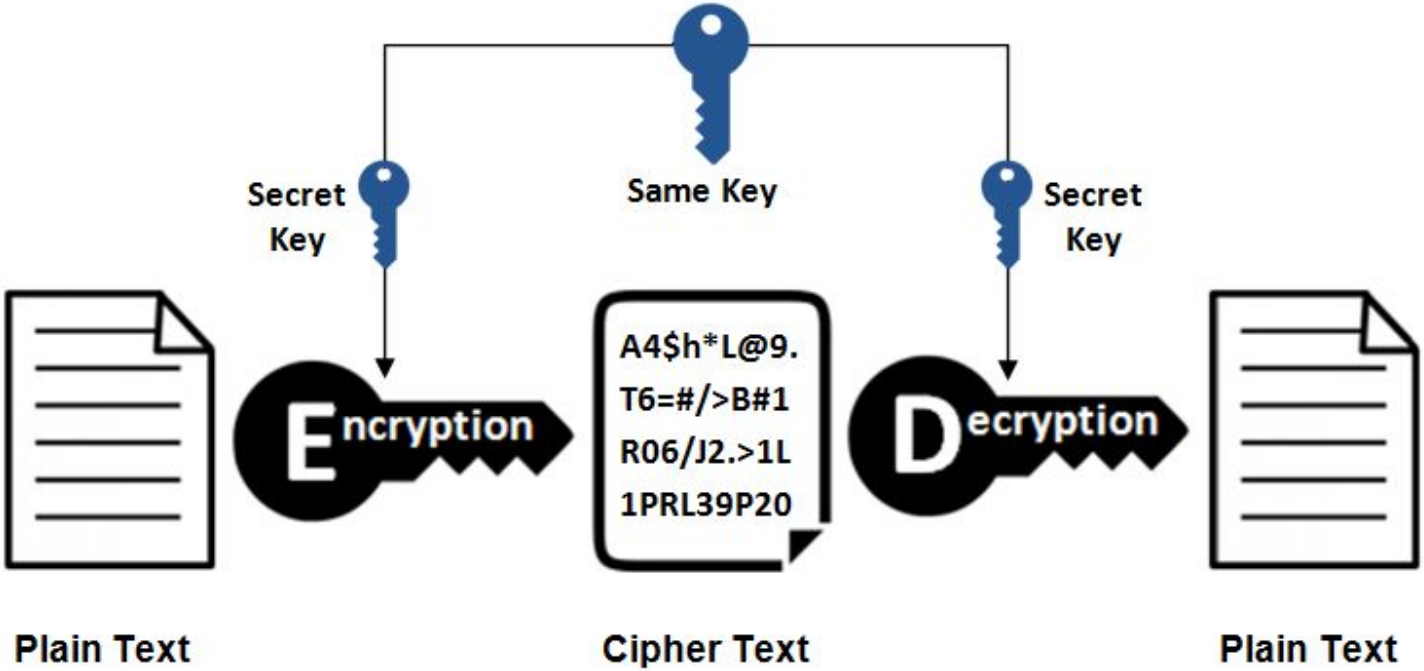
Encryption

Encryption is the process of **securely encoding data** in a way that **only authorized users with a key or password can decrypt the data to reveal the original**.

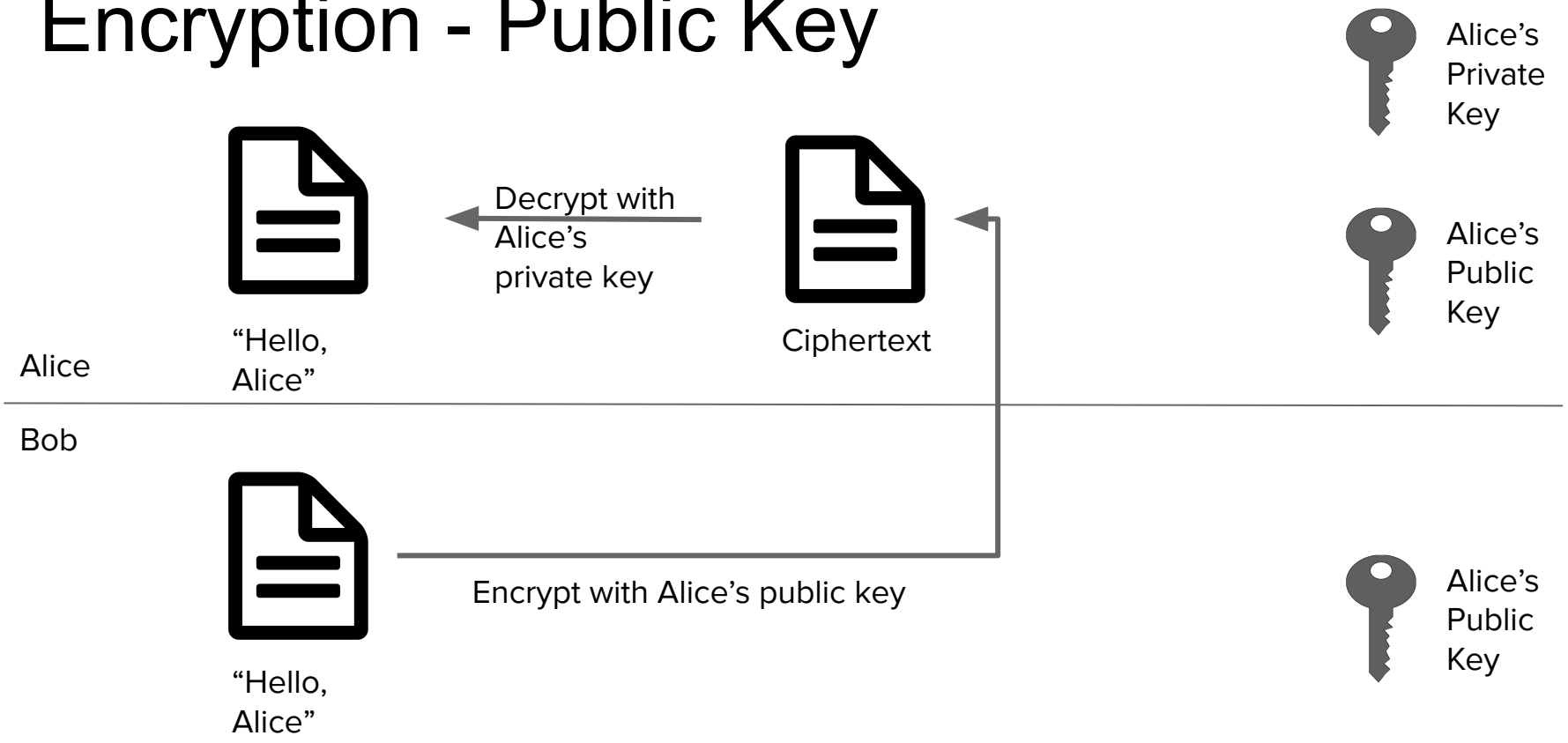
There are two basic types of encryption; symmetric key and asymmetric/ public key.

> In symmetric key, the **same key is used to encrypt and decrypt data**, like a password.
>
> In asymmetric key encryption, **one key is used to encrypt data and a different key is used to decrypt the data**.

Encryption - Symmetric Key



Encryption - Public Key



Encryption

Encryption is used when **data needs to be protected** so those without the decryption keys **cannot access the original data**.

When data is sent to a website over HTTPS it is encrypted using the public key.

While encryption does involve encoding data, the two are not interchangeable terms, **encryption is always used when referring to data that has been securely encoded**. Encoding data is used only when talking about data that is not securely encoded.

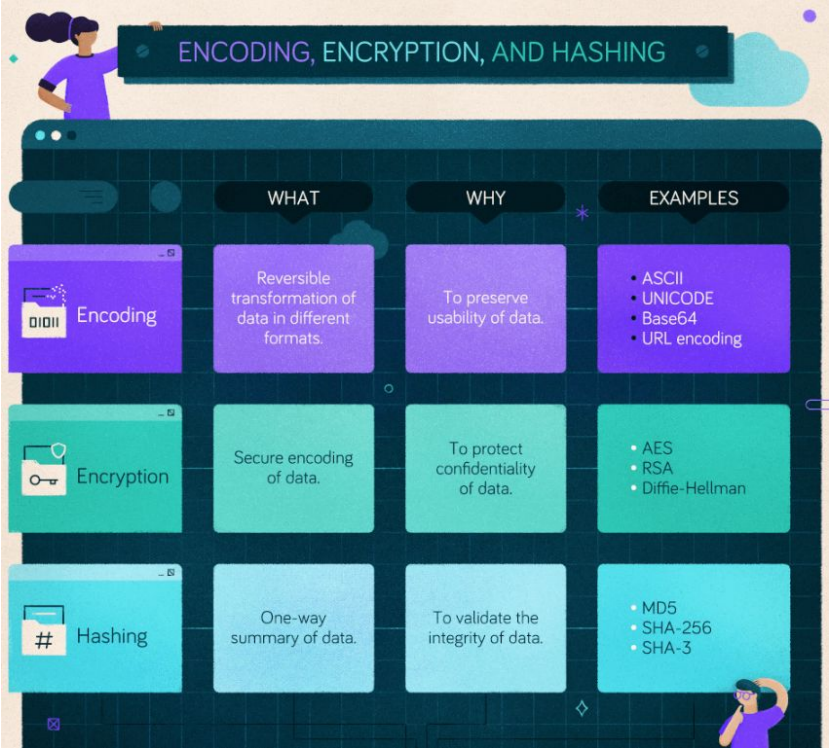
Encryption Examples

- DES Encryption (outdated)
- 3DES Encryption (not commonly used)
- AES Encryption
- RSA Encryption

Activity Time

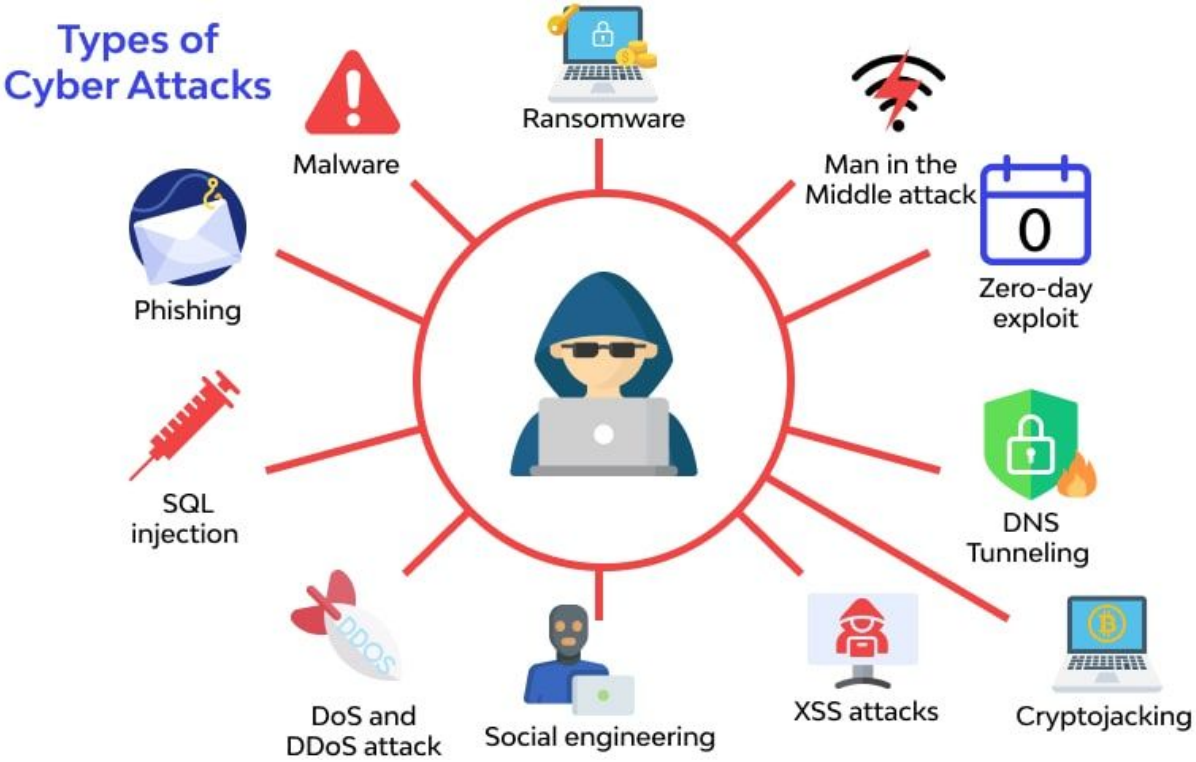
In this activity, **can you suggest some scenarios when Encryption would be used?**

Encryption Summary



Common Cyber Attacks

Cyber Attacks



Common Cyber Attacks

Backdoor Trojan

A backdoor Trojan creates a **backdoor vulnerability in the victim's system**, allowing the attacker to gain remote, and almost total, control. Frequently used to link up a group of victims' computers into a botnet or zombie network, attackers can use the Trojan for other cybercrimes.

Common Cyber Attacks

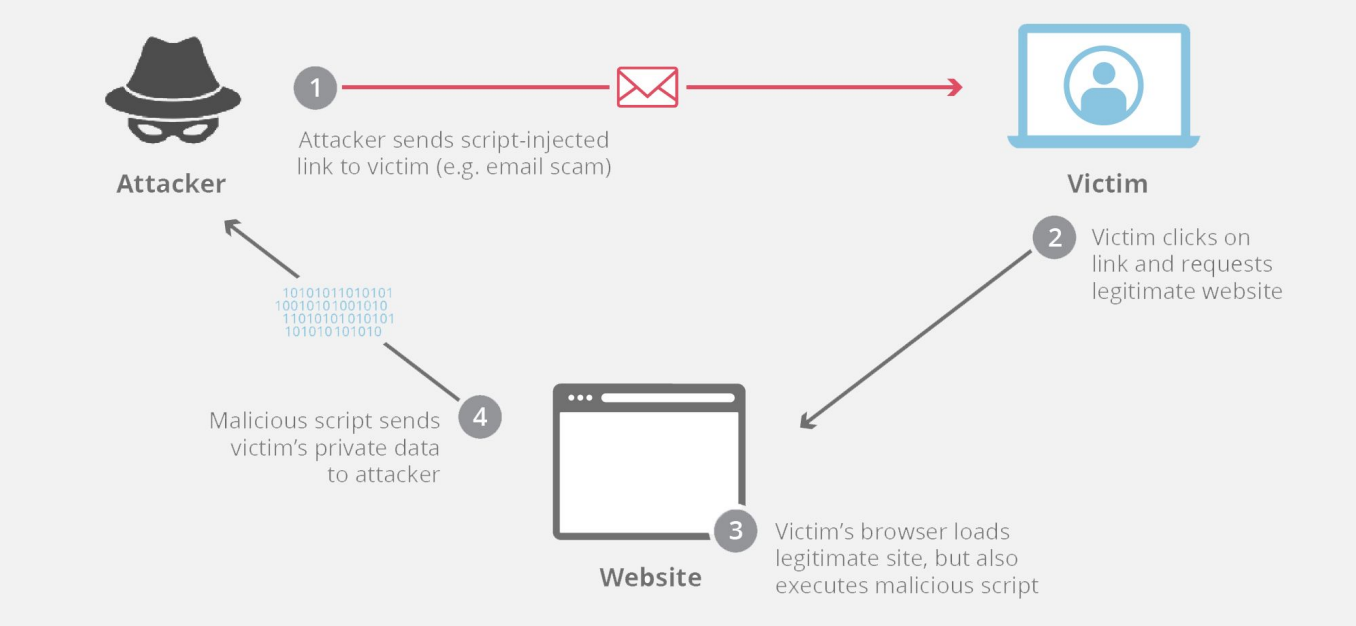
Cross-site scripting (XSS) attack

XSS attacks **insert malicious code into a legitimate website or application script** to get a user's information, often using third-party web resources.

Attackers frequently use JavaScript for XSS attacks, but Microsoft VCScript, ActiveX and Adobe Flash can be used, too.

Common Cyber Attacks

Cross-site scripting (XSS) attack



Common Cyber Attacks

Distributed Denial of Service (DDoS)

DoS and Distributed denial-of-service (DDoS) attacks **flood a system's resources, overwhelming them and preventing responses to service requests**, which reduces the system's ability to perform.

Often, this attack is a setup for another attack.

Common Cyber Attacks

DNS tunneling

Cybercriminals use DNS tunneling, a transactional protocol, to exchange application data, like extract data silently or **establish a communication channel with an unknown server**, such as a command and control (C&C) exchange.

Common Cyber Attacks

Malware

Malware is malicious software that can **render infected systems inoperable**. Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run.

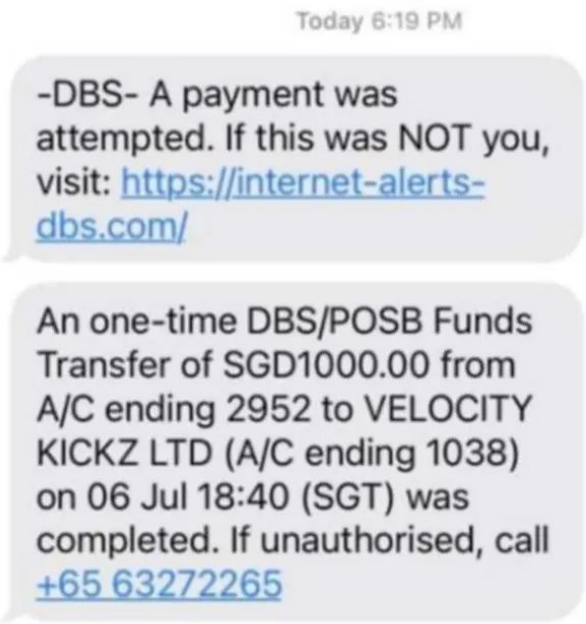
Common Cyber Attacks

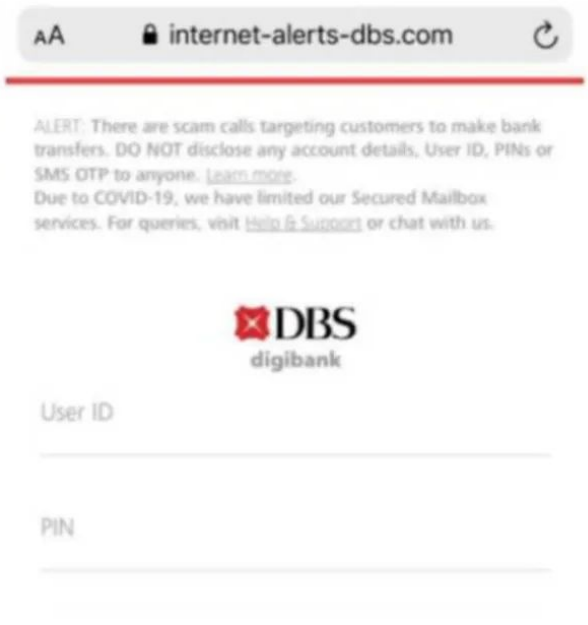
Phishing

Phishing scams attempt to steal users' credentials or sensitive data like credit card numbers. In this case, scammers send users emails or text messages designed to look as though they're coming from a legitimate source, using fake hyperlinks.

Common Cyber Attacks

Phishing





Common Cyber Attacks

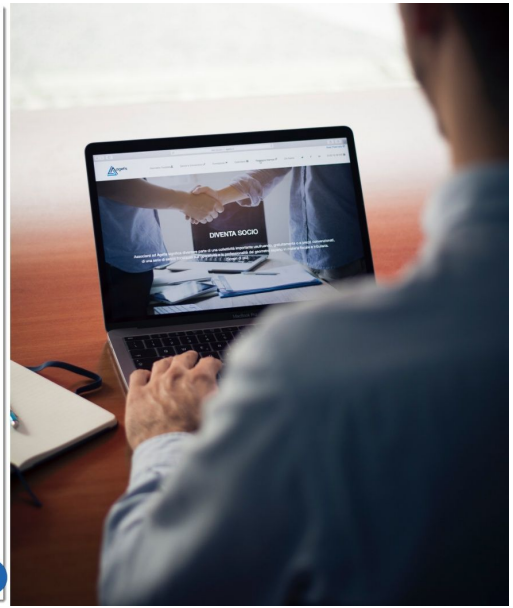
Ransomware

Ransomware is sophisticated malware that **takes advantage of system weaknesses**, using strong encryption to hold data or system functionality hostage.

Cybercriminals use ransomware to **demand payment in exchange for releasing the system**. A recent development with ransomware is the add-on of extortion tactics.

Common Cyber Attacks

Ransomware

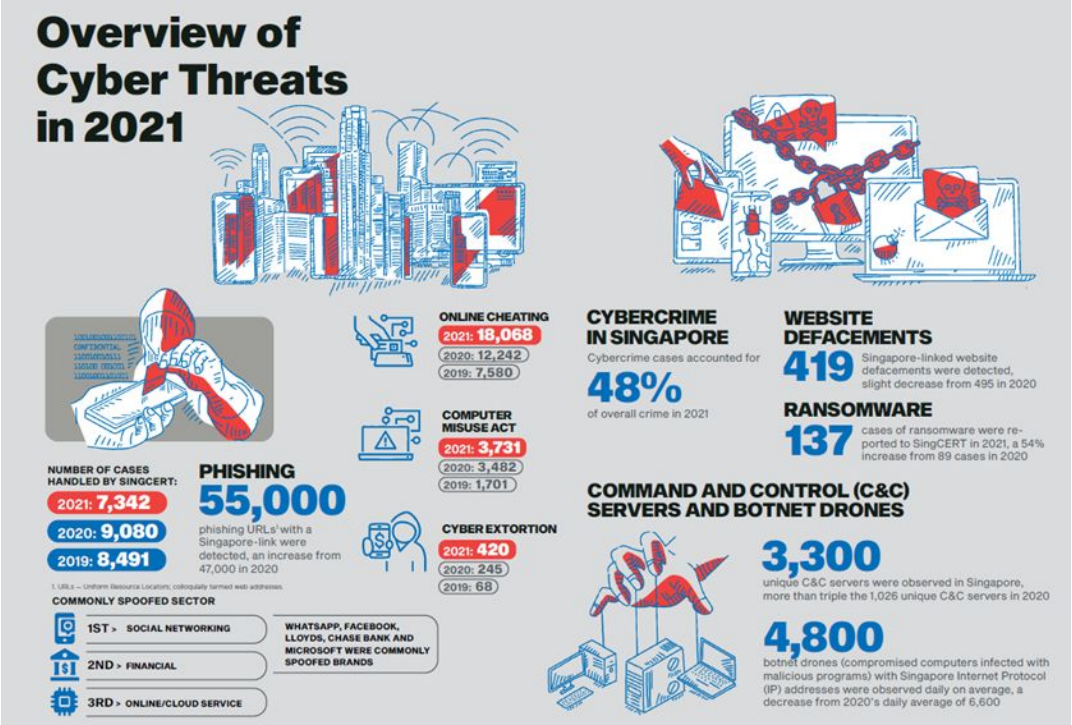


Common Cyber Attacks

SQL injection

Structured Query Language (SQL) injection attacks **embed malicious code in vulnerable applications**, **yielding backend database query results and performing commands or similar actions** that the user **didn't request**.

Common Cyber Attacks



Case Studies

Case 1: First American Financial Corporation data breach (2019)

Records affected: **885 million**

What was compromised: bank account numbers, bank statements, mortgage and tax records, social security numbers, wire transaction receipts, and driver license images

Damages: **charges from the New York State Department Financial Services (NYDFS)**

Who attacked: **no attacker**

Case 1: First American Financial Corporation data breach (2019)

Summary: This data breach was unique in the sense that there **was not a breach in the company's servers**, but an **authentication error**, meaning **no authentication was required** to view documents. There was a common web design error called Insecure Direct Object Reference (IDOR), which basically means that **anyone who searches the direct link will have access to it**. Once a single link is found, cyber criminals can use Advanced Persistent Bots (APBs) to **collect and index the remaining documents**. This error went undiscovered for years. The New York DFS alleges that First American failed to follow its own policies, neglecting to conduct a security review or a risk assessment of the flawed computer program.

Case 2: Adult Friend Finder Networks Data Breach (2016)

Records affected: **412.2 million**

What was compromised: names, email addresses, and passwords

Damages: **sensitive leaked account information**

Who attacked: **unknown**

Case 2: Adult Friend Finder Networks Data Breach (2016)

Summary: The stolen data came from **six databases with 20 years of information**. A majority of the passwords were protected by the **weak SHA-1 hashing algorithm**, which resulted in **99% of the credentials being posted by LeakSource.com** in 2016.

This data breach was particularly painful for users due to the nature of the website, which offered casual hookups and adult content.

Case 3: LinkedIn data breach (2012)

Records affected: **165 million**

What was compromised: usernames and passwords

Damages: paid **$1.25 million** to breached victims in the U.S. who paid for premium services

Who attacked: **Russian hacker**

Case 3: LinkedIn data breach (2012)

Summary: The company was attacked in 2012, when **usernames and passwords were posted to a Russian hacker forum**. The same hacker selling MySpace's data was found to be **selling individual user information** for 5 Bitcoin (roughly $5,000 in 2012). It was not until 2016 that LinkedIn revealed the full extent of the attack.

Activity Time + Break

In this activity, break into teams and pick one of the following topics:

- 2010 - WeWork Network Vulnerabilities
- 2014 - Cyber Attack on Yahoo
- 2017 - WannaCry ransomware attack.
- 2018 - A Cyber Attack on Marriott Hotels

Discuss and present a Security Vulnerabilities and Cyberattacks sharing

- What happened?
- What is the effect?
- How it did happen?
- How did they solve the problem?
- How to prevent a similar attack?

What’s Next?

Useful Links

https://www.geeksforgeeks.org/layers-of-osi-model/

https://www.geeksforgeeks.org/examples-of-tcp-and-udp-in-real-life/

https://www.liveaction.com/resources/blog/types-of-network-monitoring-protocols/