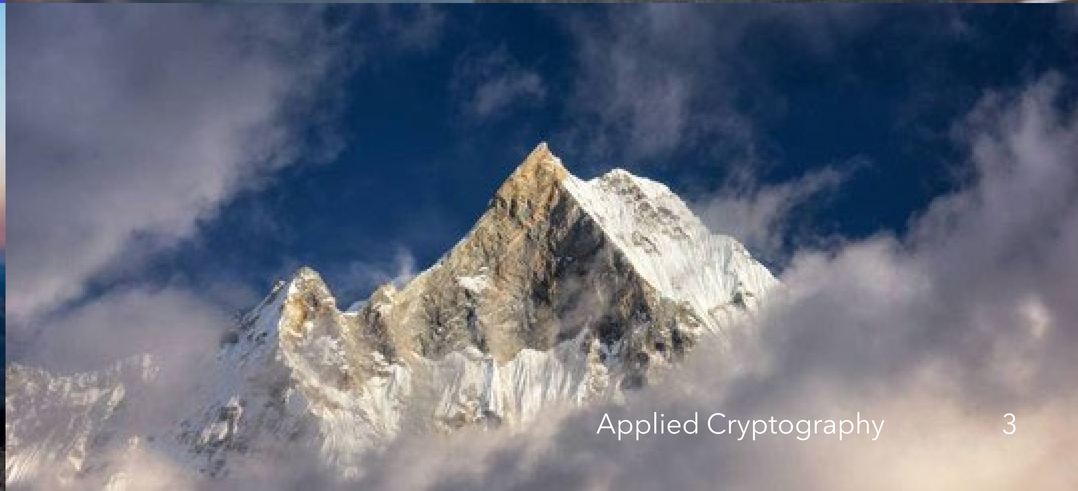
Topic 1: Introduction to Cryptography

Learning Outcome

At the end of this topic, you will be able to explain:

- The concept, terminologies, and brief history of cryptography
- Digital Security that encompasses data security and cybersecurity
- Applications of cryptography in cybersecurity

What is Cryptography? Terms and definitions

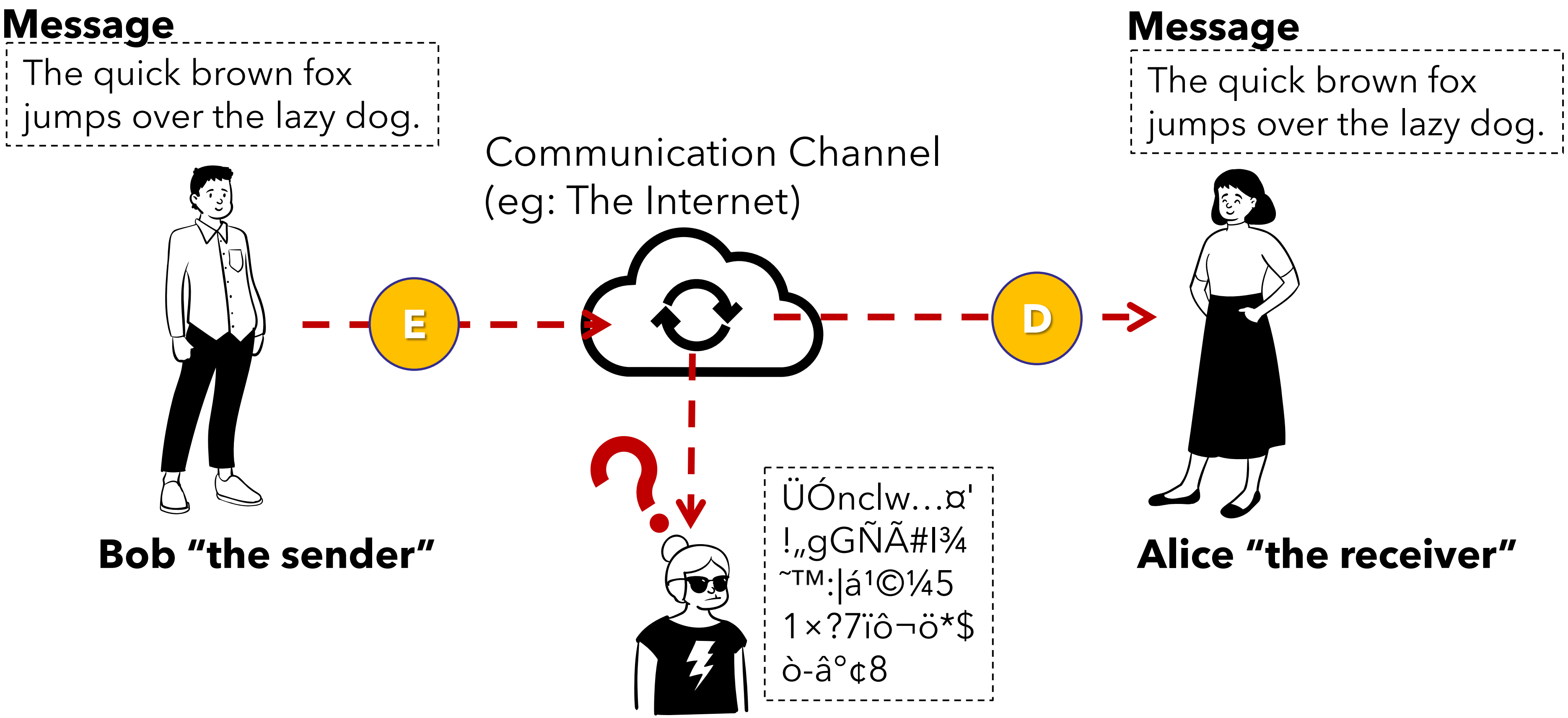


What is Cryptography?

Cryptography is the art and science of keeping data secure.

- Cryptography provides principles, means, and methods to secure the data from accessing (reading), modification (changing) by unauthorised parties either during the transmission (in motion), or in storage (at rest), and more.
- Modern cryptography exists at the intersection of mathematics, computer science, data security, electrical engineering, digital signal processing, physics, and others.

Prevent Unauthorised Access (read)



Message

The quick brown fox jumps over the lazy dog.

Communication Channel
(eg: The Internet)

Message

The quick brown fox jumps over the lazy dog.

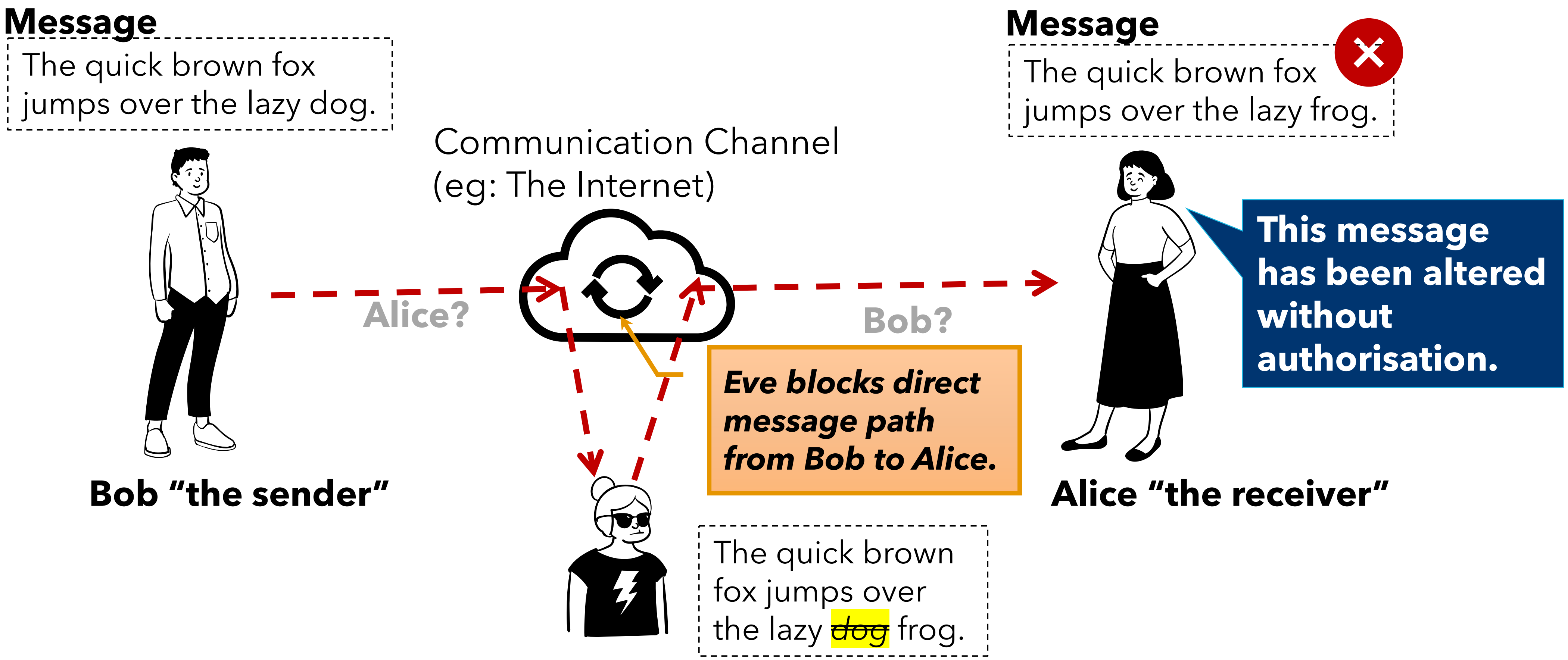
ÜÓnclw…¤'
!„gGÑÃ#I¾
˜™:|á¹©¼5
1×?7ïô¬ö*$
ò-â°¢8

Bob "the sender"

Alice "the receiver"

Eve "the eaves dropper"
Eve can intercept the messages between Bob & Alice.

Detect Unauthorised Modification



Message

The quick brown fox
jumps over the lazy dog.

Communication Channel
(eg: The Internet)

Alice?

Bob?

Eve blocks direct message path from Bob to Alice.

Message

The quick brown fox
jumps over the lazy frog.

This message has been altered without authorisation.

Bob "the sender"

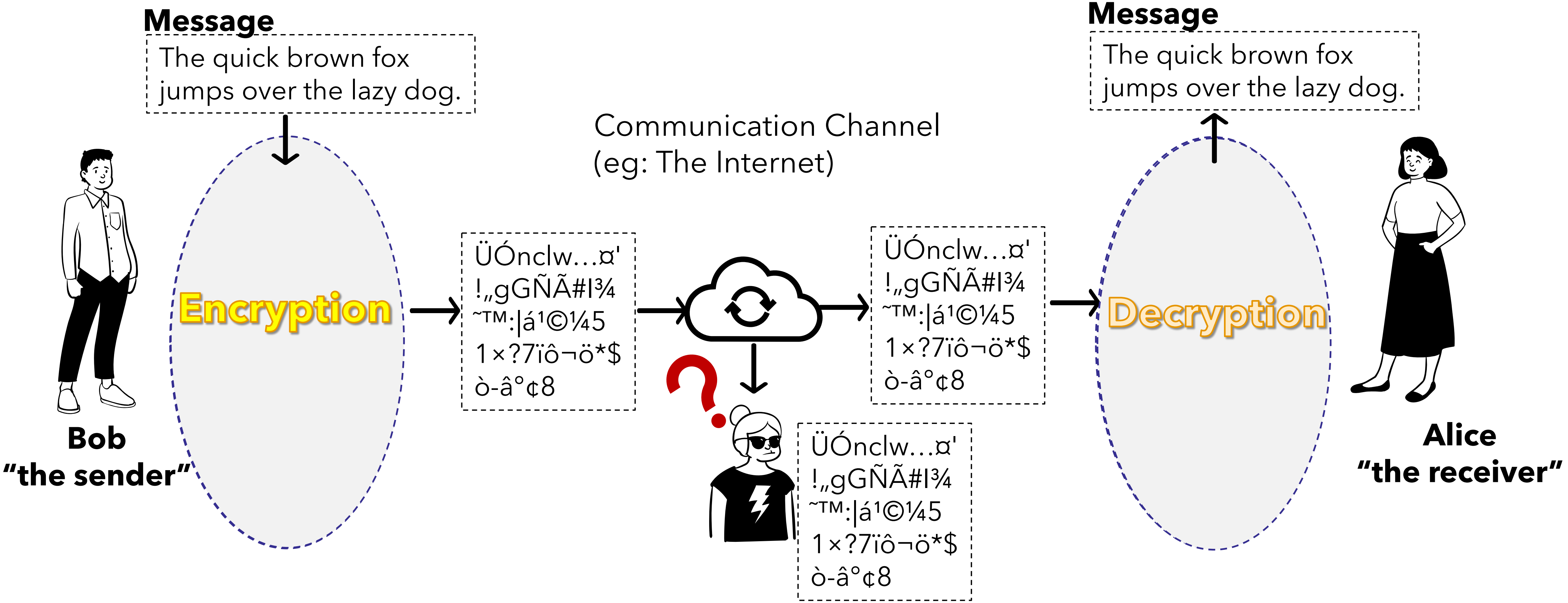
Alice "the receiver"

The quick brown
fox jumps over
the lazy ~~dog~~ frog.

Eve "the eaves dropper"

Eve can intercept the message from Bob, altered the message, and forward the altered to Alice.

Prevent Unauthorised Access (read) - Revisit



Message

The quick brown fox jumps over the lazy dog.

Encryption

ÜÓnclw…¤'
!„gGÑÃ#I¾
˜™:|á¹©¼5
1×?7ïô¬ö*$
ò-â°¢8

Communication Channel
(eg: The Internet)

ÜÓnclw…¤'
!„gGÑÃ#I¾
˜™:|á¹©¼5
1×?7ïô¬ö*$
ò-â°¢8

ÜÓnclw…¤'
!„gGÑÃ#I¾
˜™:|á¹©¼5
1×?7ïô¬ö*$
ò-â°¢8

Decryption

Message

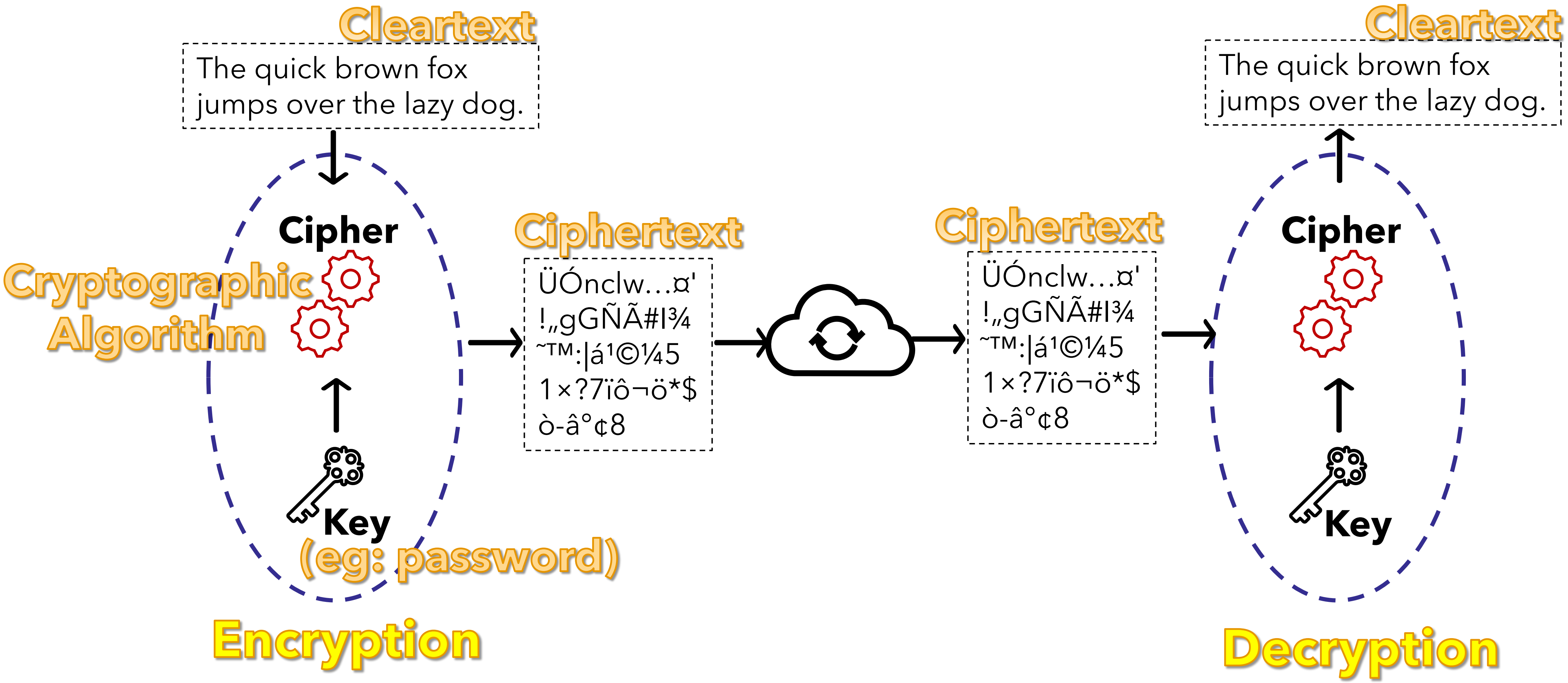
The quick brown fox jumps over the lazy dog.

Bob
“the sender”

Alice
“the receiver”

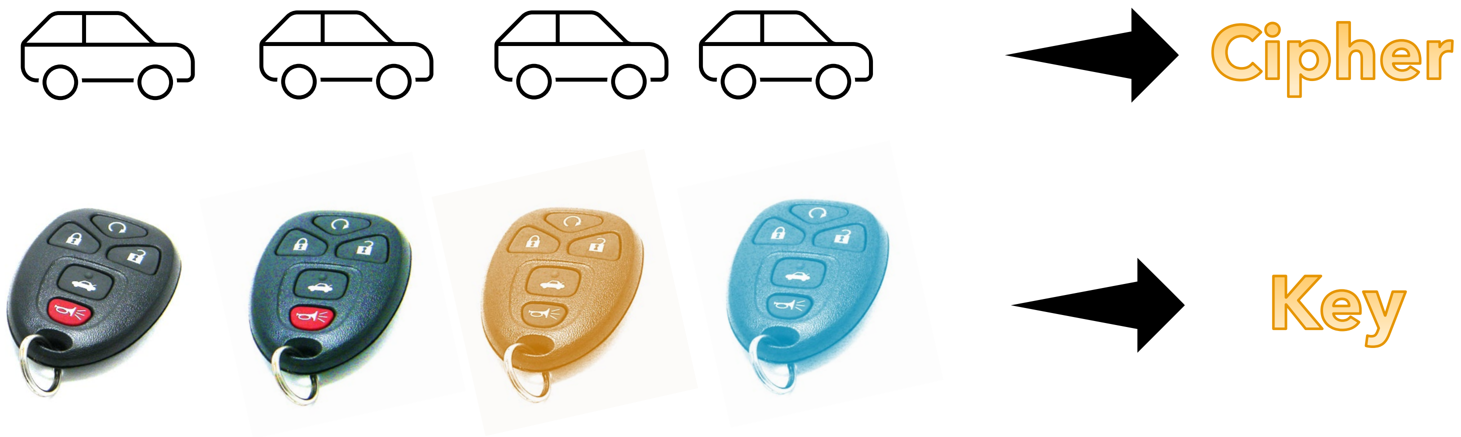
Eve “the eaves dropper”
Eve has full access to the communication but <u>not the key and possibly cipher.</u>

Terminologies



An Analogy – Cipher and Key

Cars with same model, engine, gearbox and etc.



Cipher

Key

but each with different keys…

We need both to perform cryptographic operations.

How a cryptographic key may look like …

```
B8:F0:D7:4E:FA:F3:4F:9C:FD:63:E3:C9:C5:B2:A4:5D:D9:74:EE:E0:
48:50:18:21:8E:C8:86:59:17:09:DB:9E:E2:C6:5F:06:ED:FA:39:51:
E4:38:DA:1E:28:A3:5C:38:D0:68:EA:CD:04:61:D6:CF:0D:56:B1:7B:
92:BE:4F:55:3F:D6:64:28:76:DB:BF:75:81:95:1E:2C:9B:96:26:E1:
C7:BF:BF:A0:4C:AB:82:F5:7B:2C:BA:59:C1:90:5D:F5:9B:2B:38:A7:
EF:CE:6A:04:94:FE:29:51:0E:64:56:EF:7F:22:DB:9D:40:60:DE:1F:
D2:73:84:0B:C1:99:ED:A0:DF:67:FC:4E:86:2C:34:C7:75:13:E4:AE:
FD:B3:24:EB:D9:30:66:B0:BD:7C:3C:70:13:78:12:3B:D3:2E:B2:36:
B9:D8:E5:35:F7:62:C1:39:D4:FA:8E:58:AF:C3:DD:D2:6F:28:6F:D7:
54:92:2E:85:0E:EB:28:23:9E:67:58:45:A5:0D:13:85:B2:22:76:A8:
AD:0F:BD:EA:4D:3F:07:F7:21:CC:DE:DA:D9:61:64:BB:C2:F3:25:E1:
D6:DD:D9:71:AB:5C:54:7C:E3:B3:6D:5F:B0:BF:DD:C5:B2:C2:40:76:
6A:B1:10:1C:18:7E:05:9C:ED:43:0D:D5:C2:23:A3:D3
```

Key Terminologies I

- A **cipher** (or **cypher**) is a **cryptographic algorithm** for performing **encryption** or **decryption**. We will study this in topic 2 onwards.
- The detailed operation of a **cipher** is controlled both by the **algorithm** and, *in each instance*, by a **key (**or a very complex password in general**)**.
  - Individuals use passwords
  - Computer uses keys
- The message to be communicated in its' original form is known as **clear text,** or **plain text.**
- **Encryption** is the act of scrambling the clear text into what's known as **ciphertext (** or **encrypted text)**, generally using a cipher, and a key.
- **Decryption** is reversing the encryption process – from cipher text back to the clear text.

Terminologies II

- **Cryptographers** practice cryptography
- **Cryptanalysis** is the art and science of breaking ciphertext; that is, seeing through the disguise.
- **Cryptanalysts** are practitioners of **cryptanalysis (decipher).**
- The branch of mathematics encompassing both cryptography and cryptanalysis is **cryptology,** and its practitioners are known as **cryptologists**.

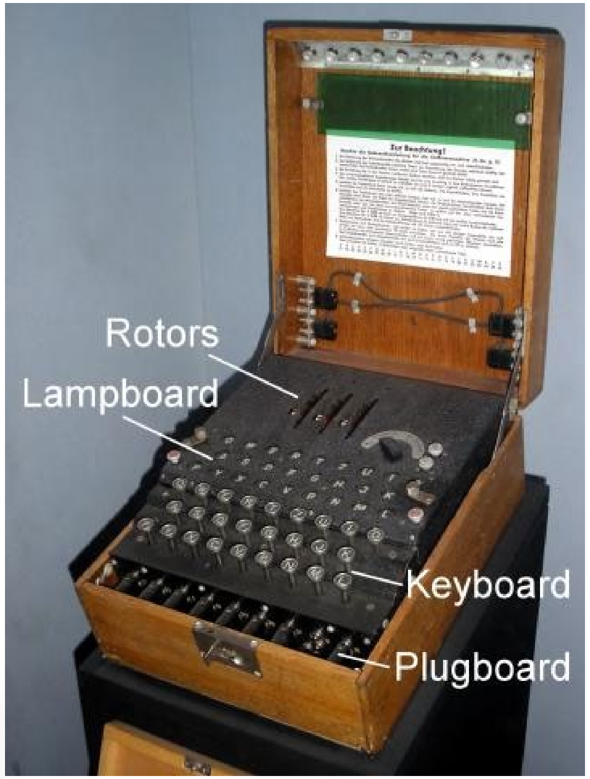
Brief History of Cryptography

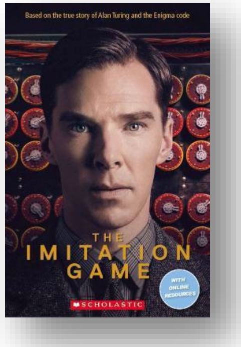
History of Cryptography

- The term “Cryptography” is derived from the Greek word ***kryptós*** (kryptos), which means hidden or secret.
- Evidence of cryptography uses has been seen in most major early civilizations.
  - Ancient Egyptians were known to use cryptographic methods in their complex hieroglyphic's writings.
  - Around 100 BC, Julius Caesar was known to use a form of **encryption**, known as **Caesar cipher** (Topic 2), to convey secret messages to his army generals posted in the war front.

History of Cryptography

- During the second world war, German forces used the **Enigma machine** *(invented by German engineer Arthur Scherbius at the end of World War I)* to secure their military communications.
  - The Enigma machine used 3 or 4 or even more rotors.
  - The rotors rotate at different rates as the sender types on the keyboard, and output appropriate letters of **cipher text**.
  - The initial setting of the rotors allows changes in encryption.
- Watch this video: https://www.youtube.com/watch?v=mcX7iO_XCFA
- Allied forces' ability to intercept and decipher the German messages proved to be the key to their victory.
- Features (with some drama) in the movie "Imitation Game".



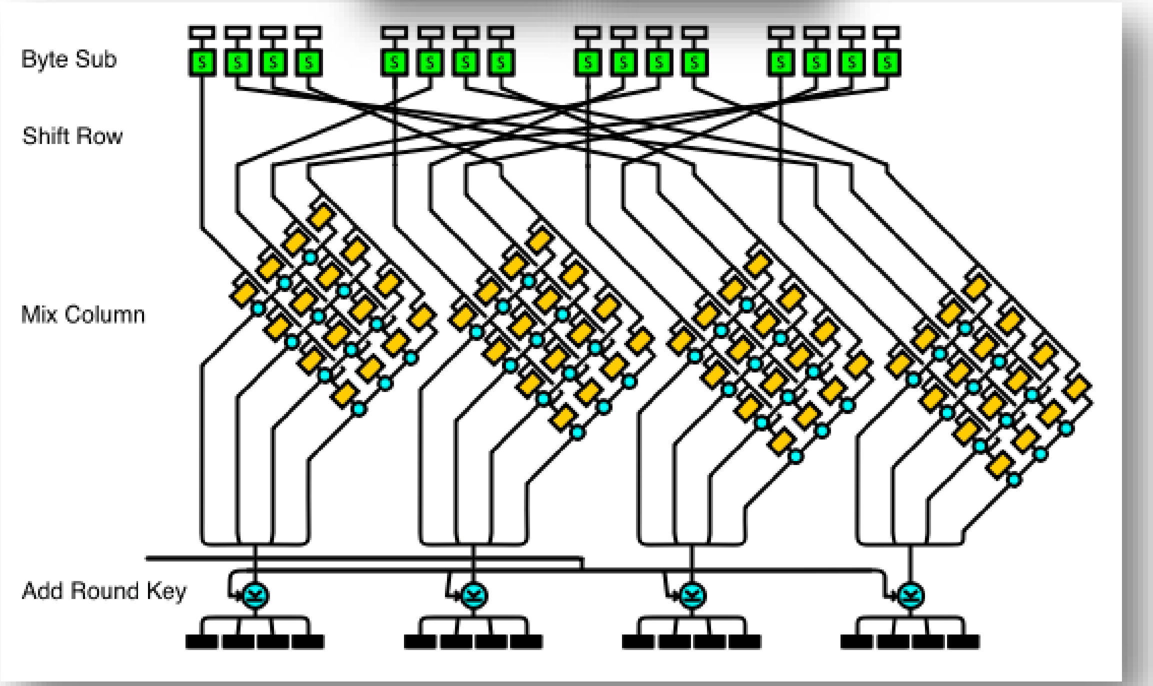


History of Cryptography

- In the early 1970s, Horst Feistel from IBM "crypto group" designed a **cipher** called **Lucifer**.
- It was recognised by then that a public review is required to make sure the cipher is sound.
- Therefore, in 1973, the Nation Bureau of Standards in the US (now called NIST) put out a request for proposals for a **block cipher** (Topic 3 & 4) which would become a national standard.
- Lucifer was eventually accepted and was called **DES or the Data Encryption Standard** (Topic 3).

History of Cryptography

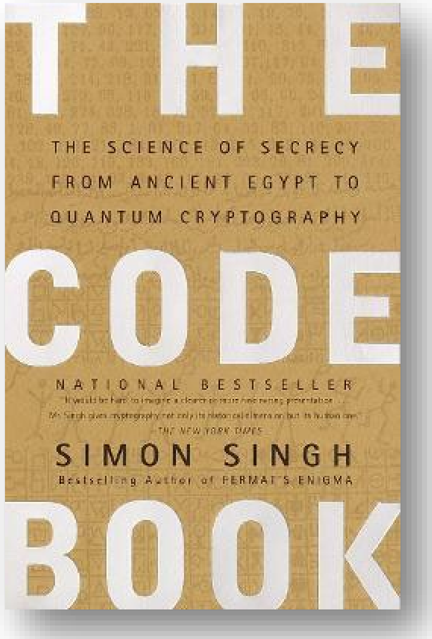
- In 1997, NIST again put out a request for proposal for a new **block cipher** (Topic 3). It received 50 submissions.
- In 2000, it accepted **Rijndael**, developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and named it as **AES** or **the Advanced Encryption Standard** (Topic 3), which is widely used today.
- We will visit the development of "Asymmetric cipher" in the beginning of the computing era in topic 4.
- Read more about history of cryptography at https://en.wikipedia.org/wiki/Cryptography.



Ref: https://lib.rs/crates/aes

History of Cryptography

- Wanted to know more? A good text you may read in leisure..
- **The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography**, ISBN-10 : 0385495323



Applications of Cryptography

Application of Cryptography

- Cryptography can be applied to many disciplines.
- In this module, we will focus our study on how cryptography is applied in the domains of **digital security**.
- **But first, what is digital security?**
- It comprises of
  - **Cybersecurity**, and
  - **Data (or) Information Security**
- Both are usually referred together as "**cybersecurity**".
- Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

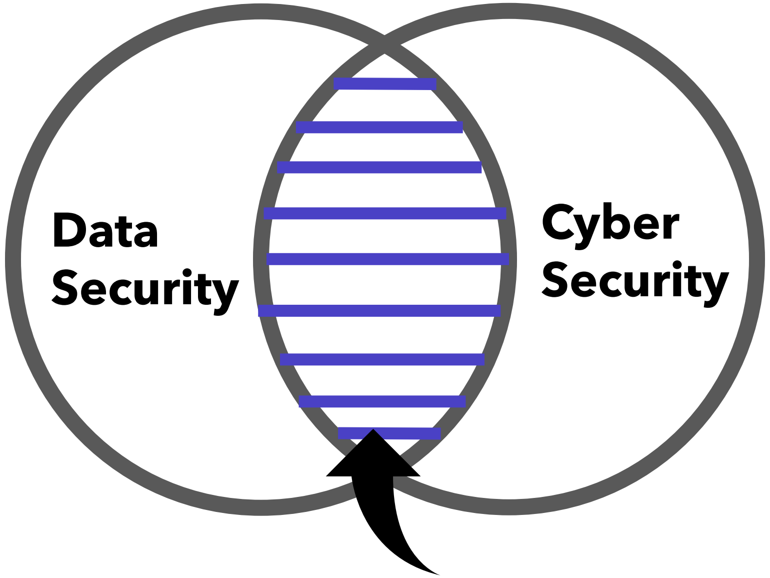
Pillars of Cybersecurity (CIA)

Three pillars of cybersecurity are:

- **Confidentiality**
  - Prevent unauthorised access to data/information and systems
- **Integrity**
  - Prevent unauthorised alternation to data/information and systems
- **Availability**
  - Ensure data and systems are consistently available when needed

Cyber and Data Security Relationship

Data Security
Maintain the confidentiality, integrity and availability of **data**.



Cybersecurity
Maintain the confidentiality, integrity and availability of **systems**.

Cybersecurity and data security overlapped for digital data. Non-secure ICT systems will increase the risk of data security breaches.

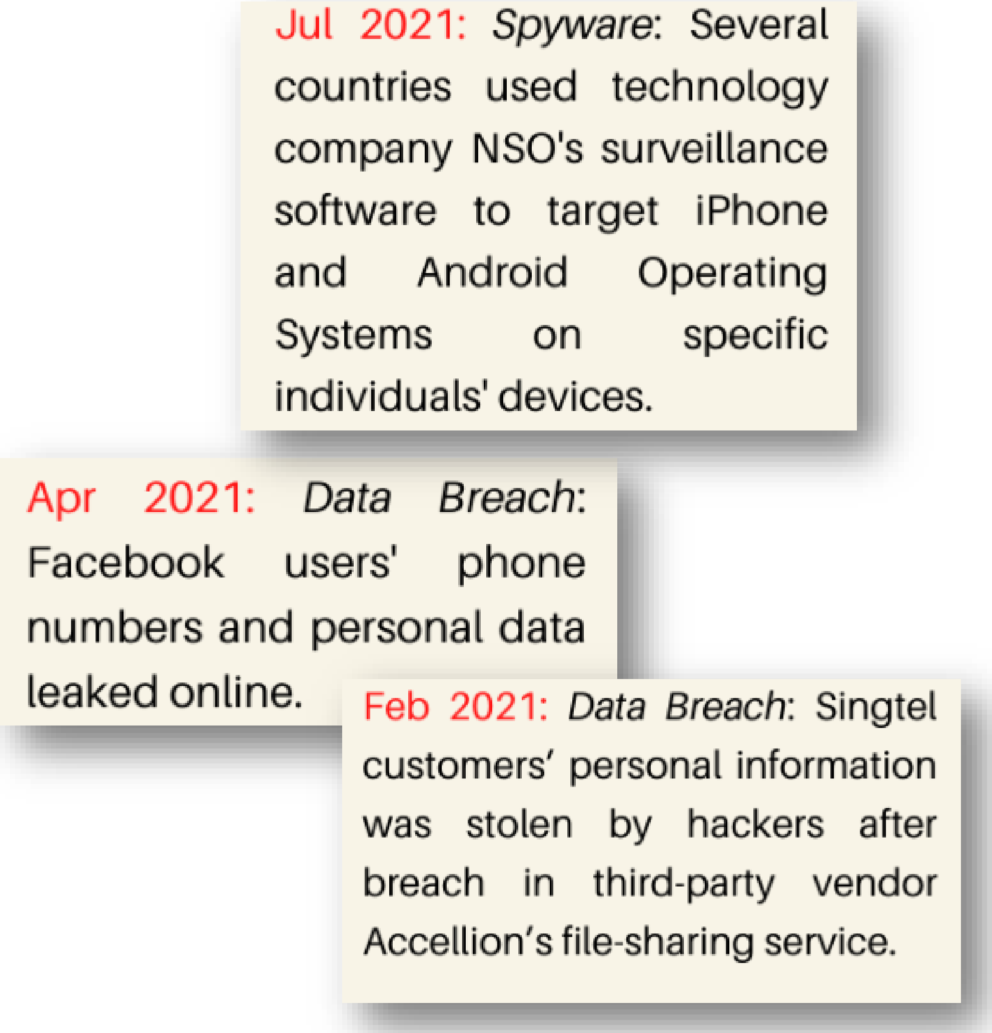
We will use the term cybersecurity to cover both data and cybersecurity from here.

Importance of Data Security

- Data (or) information is the lifeblood of the digital economy, society and government.
- Data is used and shared among various entities, stake holders for improved revenue, products, and services.
- Data/Information security is about **protecting the organization and personal data, and preserve the privacy of individuals**.
- Data must be protected from abuses, misuses and destruction by the malicious parties.

Importance of Data Security

- Cyber-criminals stole, destroy, misuse or abuse victim organisations' important data, and disrupt the functioning systems.
- Leak of personal data can lead to undesired consequences to the privacy of individuals.
- These intrusion and disruption events are called **cyber-incidents**.
- The cyber-incidents incurred monetary and reputational losses to the affected organisations.



Jul 2021: *Spyware*: Several countries used technology company NSO's surveillance software to target iPhone and Android Operating Systems on specific individuals' devices.

Apr 2021: *Data Breach*: Facebook users' phone numbers and personal data leaked online.

Feb 2021: *Data Breach*: Singtel customers' personal information was stolen by hackers after breach in third-party vendor Accellion's file-sharing service.

Cryptography applications for CIA

- **Confidentiality**
  - Prevent unauthorised access to information and systems
  - **Encryption & decryption (topic 2, 3 & 4)**
- **Integrity**
  - Prevent unauthorised alteration to data and systems
  - **Message digest, digital signature and PKI (topic 5 & 6)**
- **Availability**
  - Ensure data and systems are consistently available when needed
  - **No direct application of cryptography**

Cryptography Applications

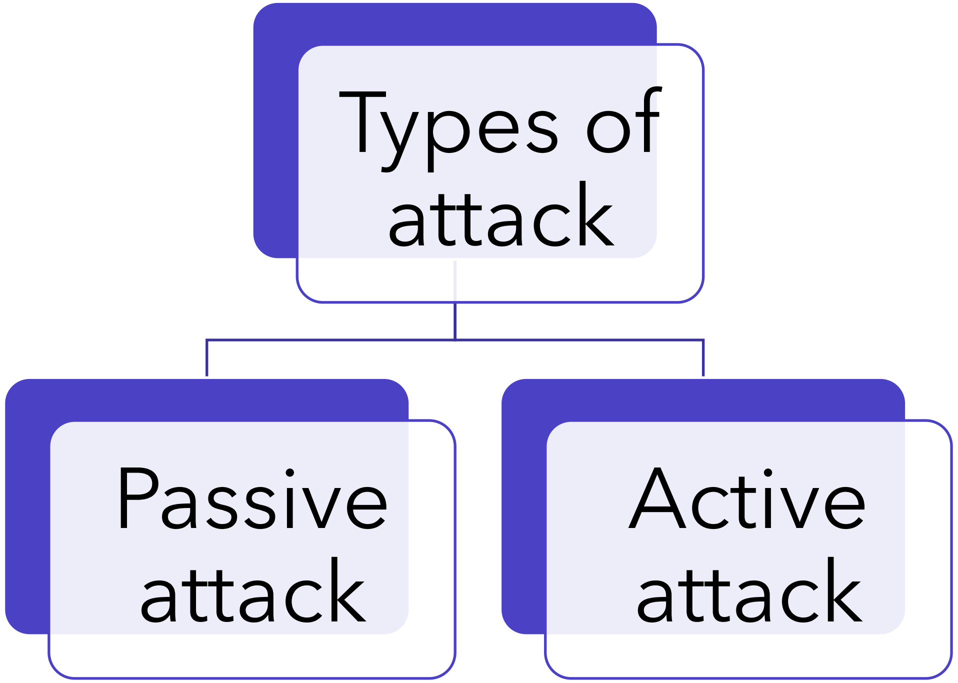
Cryptography is also tasked to do the following important functions:

- **Authentication**
- It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.
- **Nonrepudiation**
- A sender should not be able to falsely deny later that he sent a message.

Types of Attacks on Message Communications

Types of Attacks on Communication

There are two types of attack to the security of data – passive and active attack.

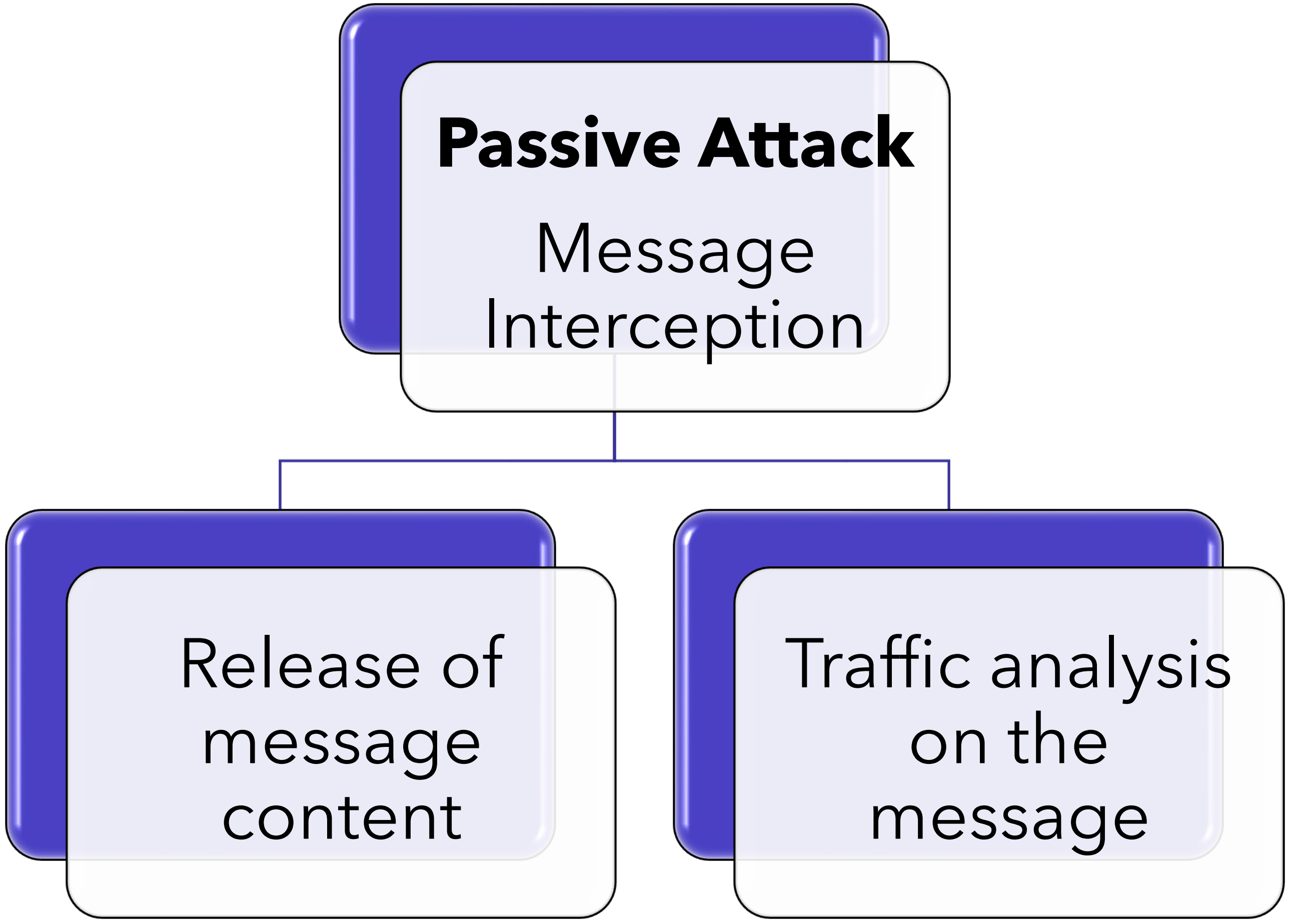


Types of attack

Passive attack

Active attack

Types of Attacks – Passive Attack



Passive Attack

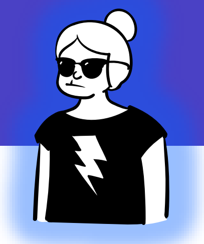
Message Interception

Release of message content

Traffic analysis on the message

Attack on message confidentiality

Types of Attacks – Passive Attack



Passive attack targets the message **confidentiality.**

- This attack intercept and captures the message (partial or full) via eavesdropping or monitoring of communication
- The attacker can
  - release the message content to the unauthorised third parties.
  - If the message is scrambled (encrypted), that attacker may try to figure out the original (clear text) of the message. This is known as **cryptanalysis**.
- The attacker does not attempt to change the message content in this attempt.
- Passive attacks are hard to detect.

An example: **Spyware**

- A surveillance software that targets iPhones and Android devices
- Once installed without authorization, it can syphon the data such as text messages, calls, and other information stored on the device to the third parties

Passive Attack Example with Eve

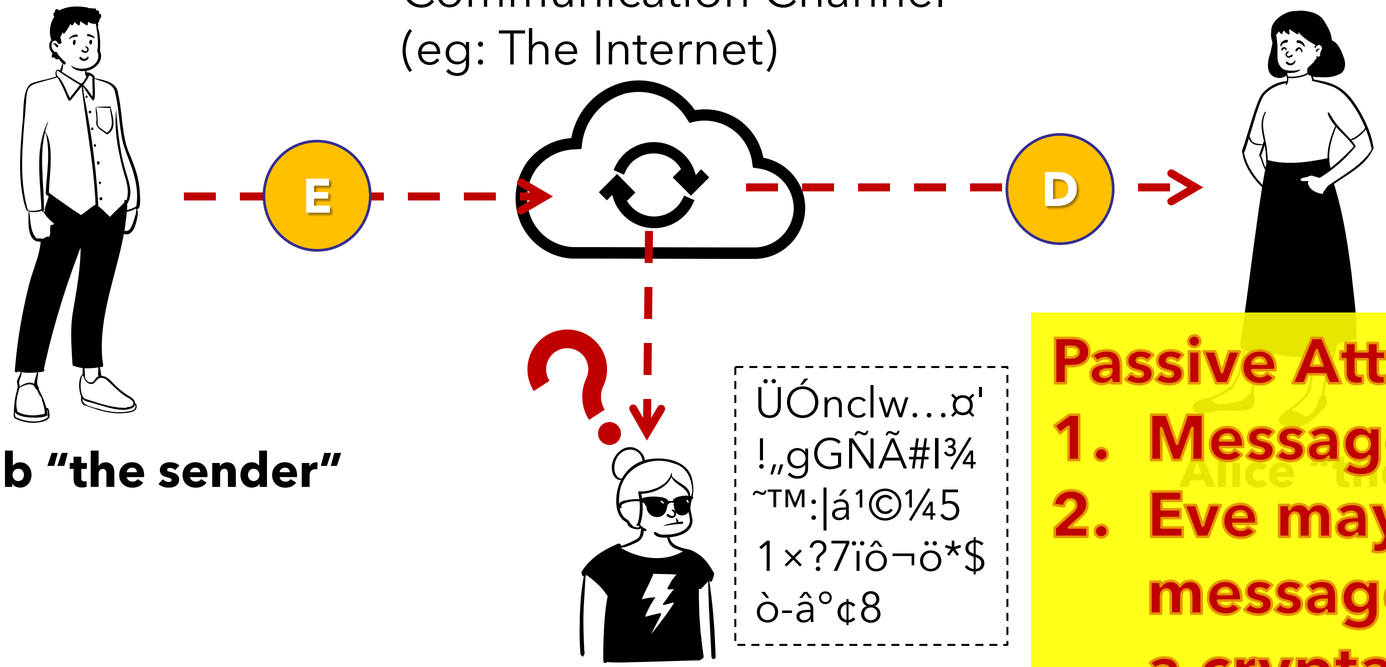
Message

The quick brown fox
jumps over the lazy dog.

Communication Channel
(eg: The Internet)

Message

The quick brown fox
jumps over the lazy frog.



Bob "the sender"

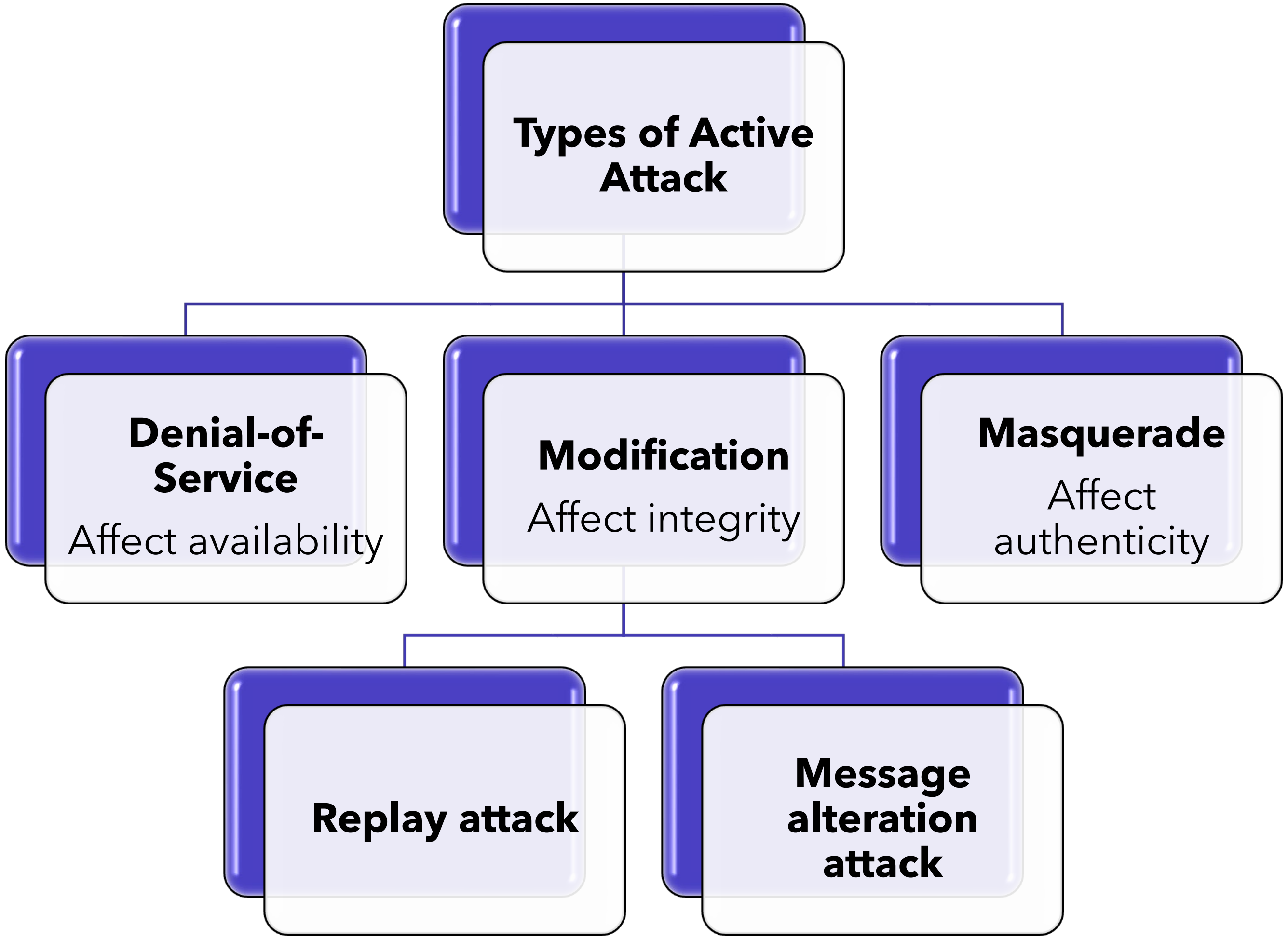
ÜÓnclw…¤'
!„gGÑÃ#l¾
˜™:|á¹©¼5
1×?7ïô¬ö*$
ò-â°¢8

Eve "the eaves dropper"
Eve can intercept the messages between Bob & Alice.

Passive Attack

1. **Message Interception**
2. **Eve may release the message and/or attempt a cryptanalysis to decipher the message.**

Types of Attacks – Active Attack



Types of Active Attack

Denial-of-Service

Affect availability

Modification

Affect integrity

Masquerade

Affect authenticity

Replay attack

Message alteration attack

Attack on message confidentiality & integrity.

Types of Attacks – Active Attack

- In contrast to a passive attack, an active attack involves interception and modification to the contents of the original message.
- There are 3 sub-categories of an active attack:

1. **Denial-of-service (or) Interruption attack**
   - Denial-of-service (DOS) attacks try to prevent legitimate users from accessing services which they are eligible for.
   - Example: The attacker(s) send large network traffic to overwhelm the victim server.
2. **Modification attack**
   - Example: An attacker (Eve) change the recipient of the fund from the legitimate receiver (Alice) to herself.
3. **Masquerading (or) Impersonation attack**
   - An entity poses as another entity.
   - Example: Eve impersonates Alice and sends messages to Bob.

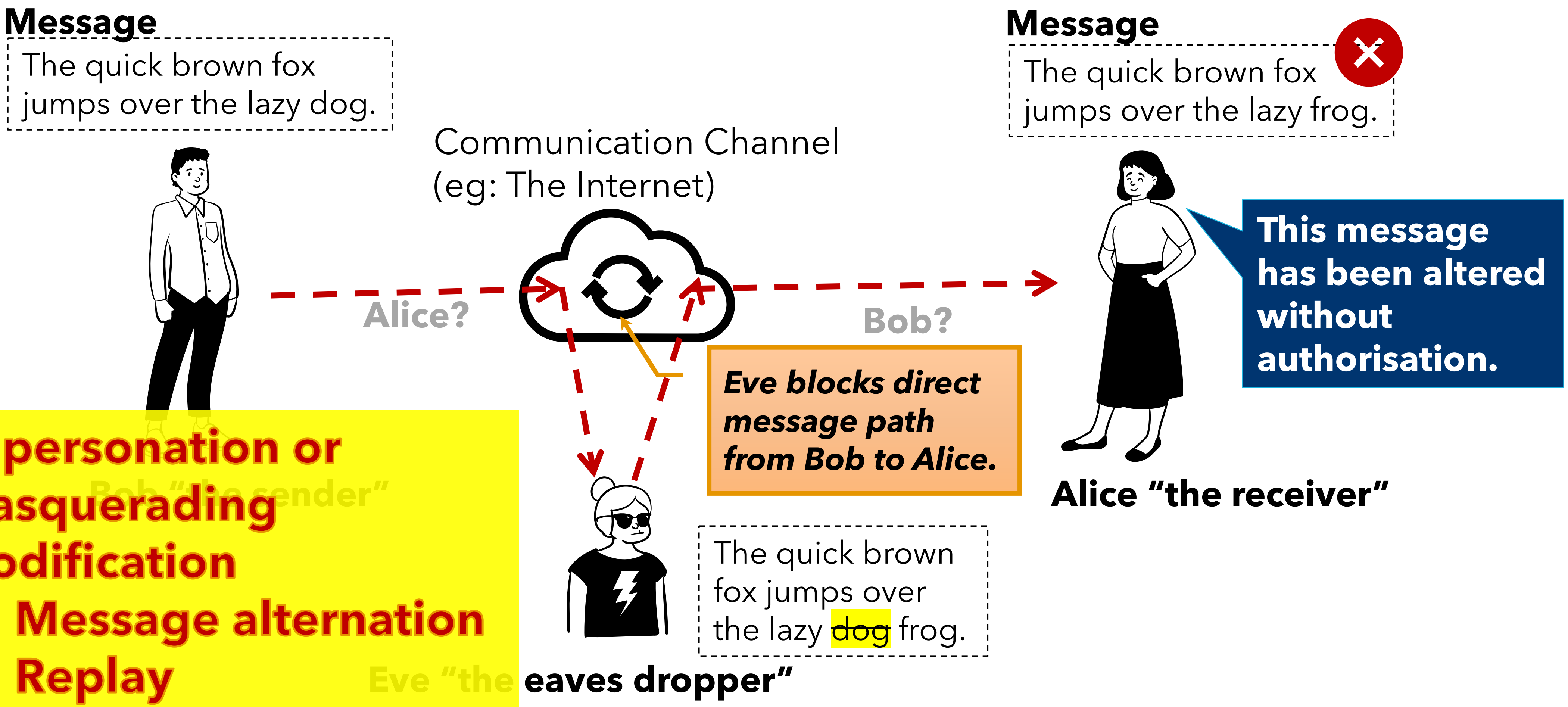
Example – A Replay attack

- A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what he/she wants.
- **Example**:
- Suppose Alice wants to prove her identity to her bank for a financial transaction.
- The bank requests her "encrypted" password as proof of identity, which Alice provides.
- Eve is eavesdropping on the conversation. She intercepts them and keeps the Alice encrypted password.
- Later, Eve (acting as Alice) connects to the bank.
- When asked for proof of identity, Eve sends Alice's encrypted password which she obtained from the previous session. The bank accepts, thus granting Eve access to Alice's account.

Example – A Message Alternation Attack

- In a message alteration attack, an attacker intercepts the network communication, captures and modifies the message, and replays it to his/her advantage.
- **Example**:
- Suppose Bob sends a message to his bank to transfer $1000 to Alice's account.
- Eve eavesdrops on secure communication. She is able to capture the message. Eve, and modifies the message to transfer $10,000 to her account instead.
- Bank assumes that the message is coming from Bob and proceed to execute the transfer.
- Note that both the beneficiary and the amount have been changed. Only one of these could have also caused an alteration of the message.
- This attack is difficult to prevent but easy to detect (topic 4).

Active Attack Example with Eve



Message

The quick brown fox jumps over the lazy dog.

Communication Channel (eg: The Internet)

Message

The quick brown fox jumps over the lazy frog.

This message has been altered without authorisation.

Eve blocks direct message path from Bob to Alice.

Alice "the receiver"

Bob "the sender"

The quick brown fox jumps over the lazy ~~dog~~ frog.

Eve "the eaves dropper"

1. **Impersonation or Masquerading**
2. **Modification**
   - **Message alternation**
   - **Replay**

Eve can intercept the message from Bob, altered the message, and forward the altered to Alice.

Our learning journey …

- Cryptography can provide the answers to these nature of network attacks – and more.
- Lets' find out how it works in the subsequent topics.

Summary

- Cryptography is the art and science of keeping data secure.
- Cryptography can be applied in various domains including cybersecurity.
- Confidentiality, Integrity, and availability are three main pillars of cybersecurity, also known as the CIA triad.
- Cryptography is used in the cybersecurity domain to preserve confidentiality, integrity, authenticity, and non-repudiation.
  - Encryption and Decryption aim to provide the confidentiality of data.
- Two types of network attacks are passive and active attacks.