

<https://github.com/jiportilla/crypto101>

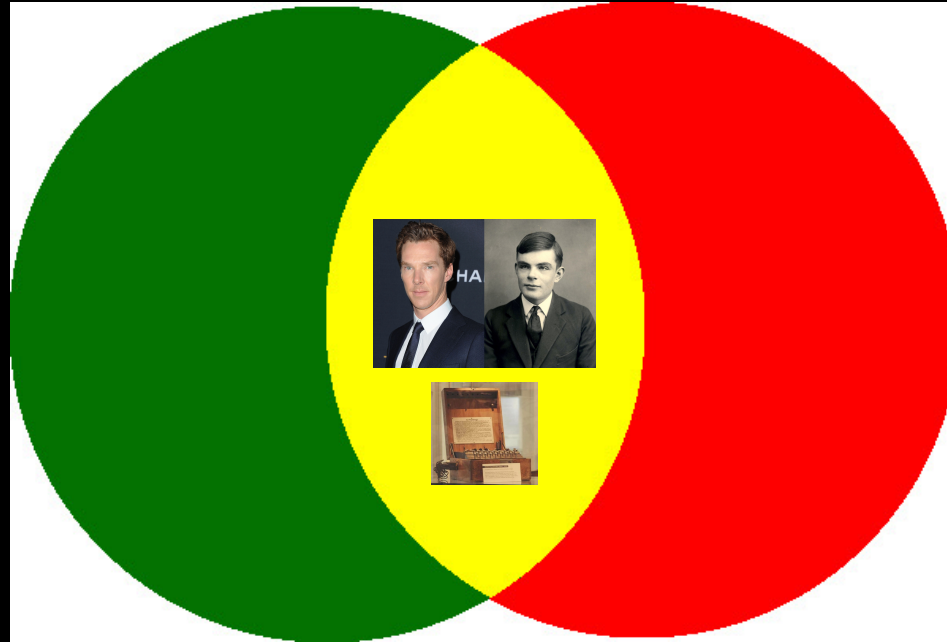
Cryptography 101

Hands on lab

- Ivan Portilla
- AI Leader
- ivanp@us.ibm.com
- 01/23/2022



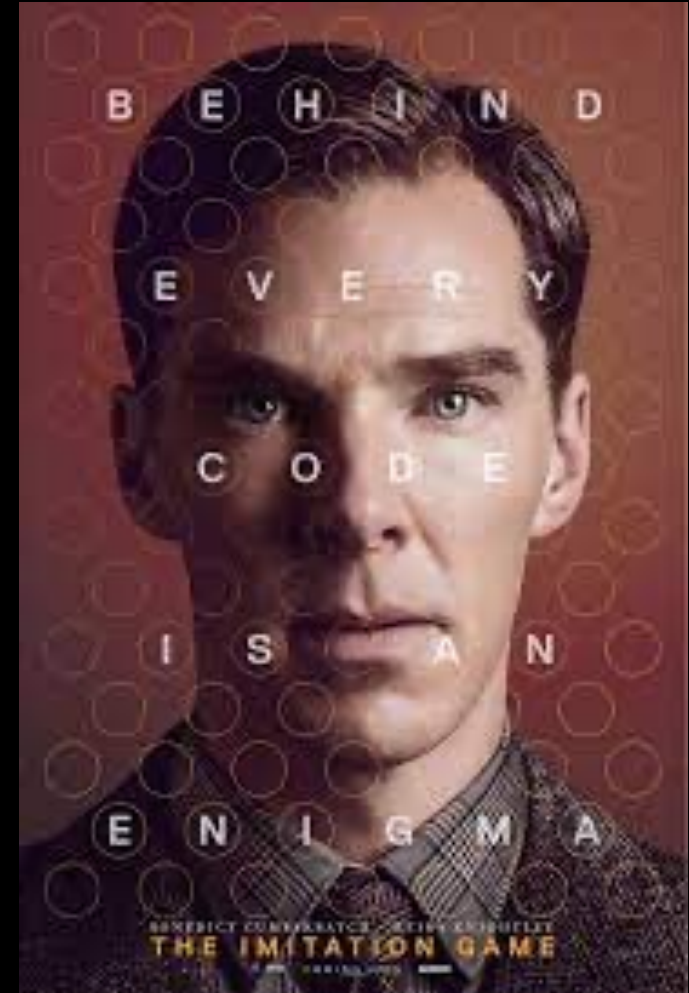
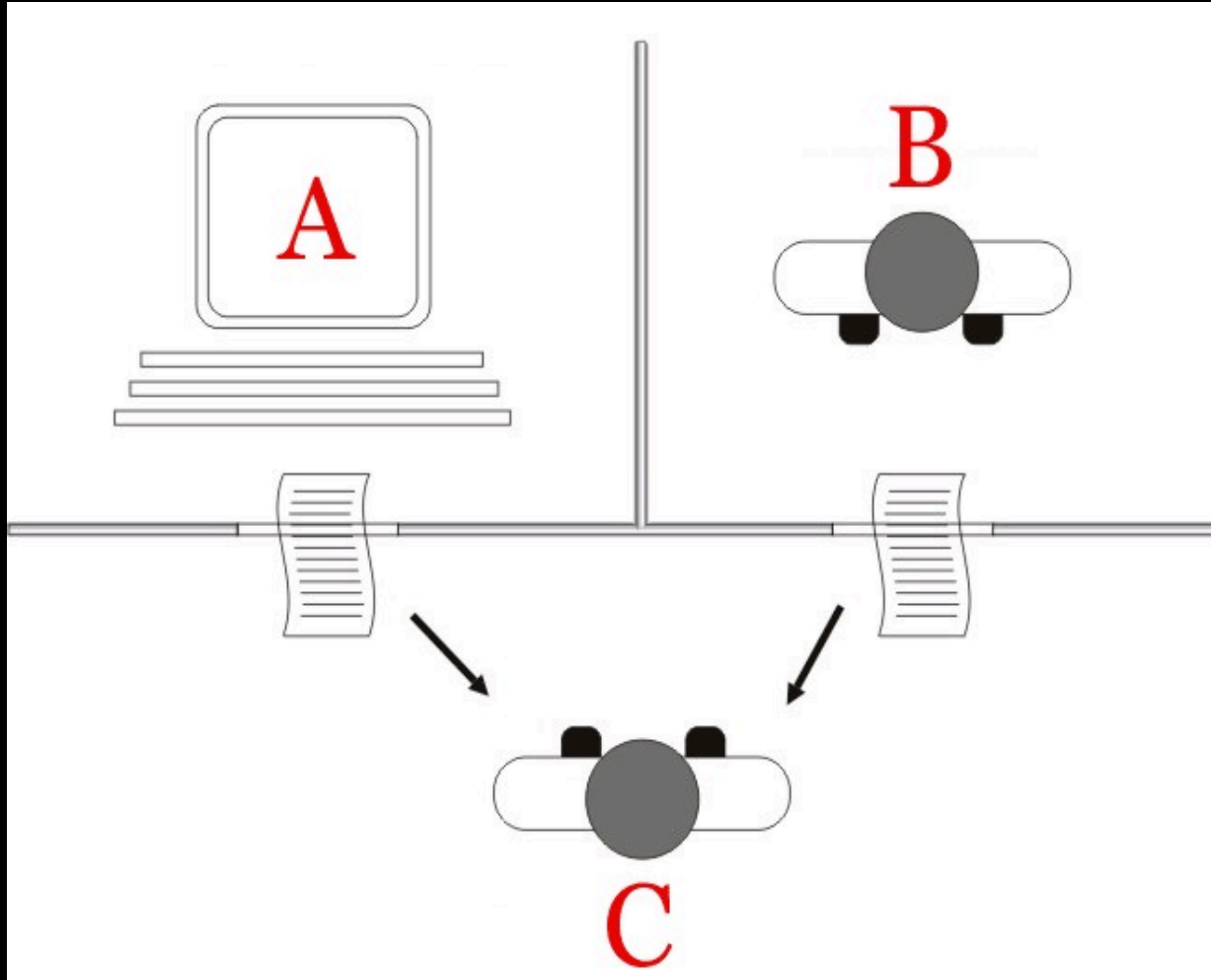
Artificial
Intelligence



Cryptography

<https://bletchleypark.org.uk/>

Class Exercise



ALAN TURING'S OFFICE

Here at his desk in Hut 8, Turing took the lead on breaking naval Enigma ciphers – something few thought could ever be done. His mathematical skills also enabled him to break other ciphers, including the complex Lorenz cipher where he used a method that became known as Turingery. Together with his fellow Codebreaker Gordon Welchman, he developed the Bombe machine to help speed up the codebreaking process.

IN THEIR WORDS

If anyone was indispensable to Hut 8 it was Turing. The pioneer work always tends to be forgotten when experience and routine later make everything seem easy, and many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realised by the outside world.

Hugh Alexander, Codebreaker, Hut 8



<https://bletchleypark.org.uk/>



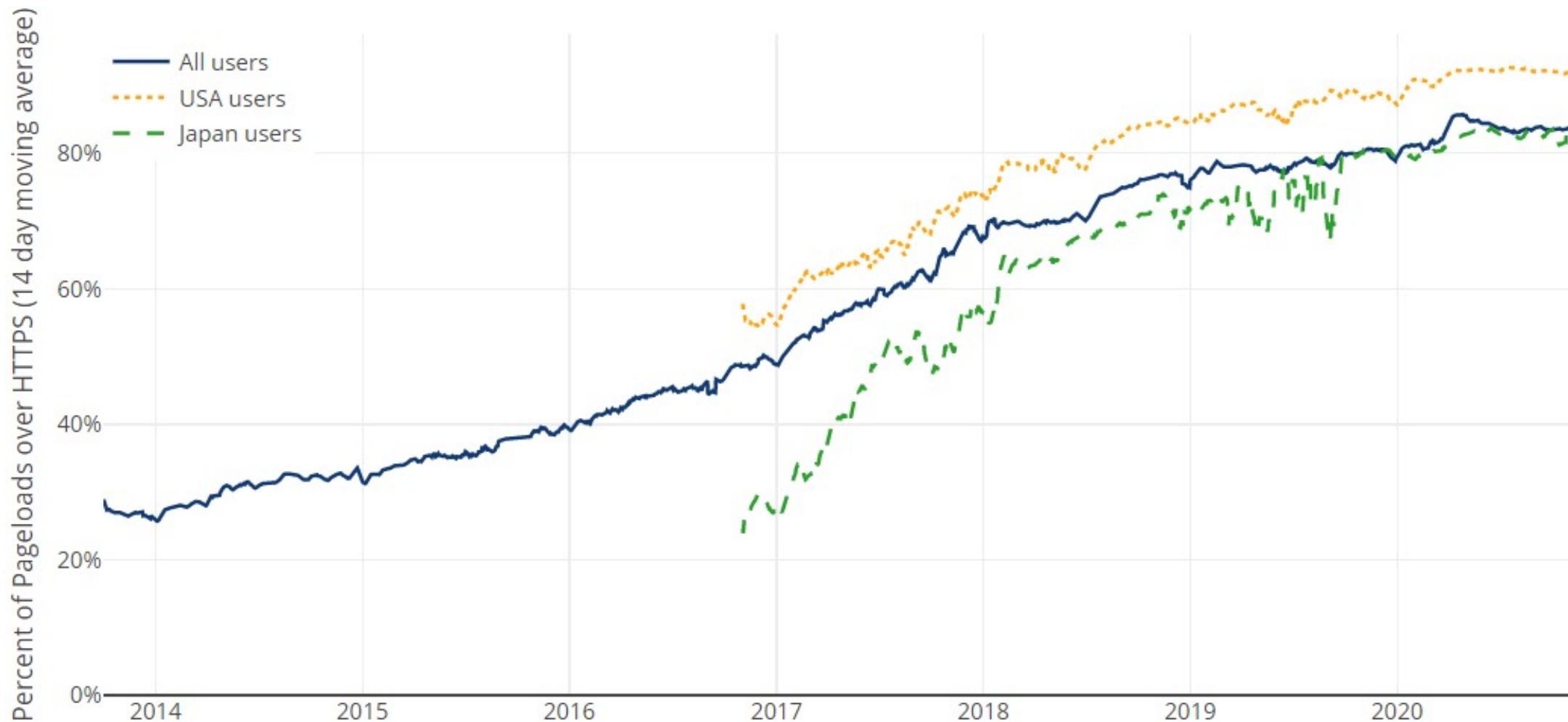
What is cryptography?

Secret messages using math / algorithms.

Today, cryptography is used to control **who** can **see** certain **information**, and also guarantees the **authenticity** of it.

HTTPS used in Firefox

(14-day moving average, source: [Firefox Telemetry](#))



What is cryptography?

The word cryptography comes from Greek:

crypto secret
graphy writing


Encryption

Using a **secret** to convert **cleartext** into **ciphertext** data that, without the secret, is meaningless.

“pepper”  **encrypt**(“pepper”, secret)



“|🧊9!^%”

decrypt(secret) “|🧊9!^%”  “pepper”

Hashing vs Encryption

Hashing is used to validate data

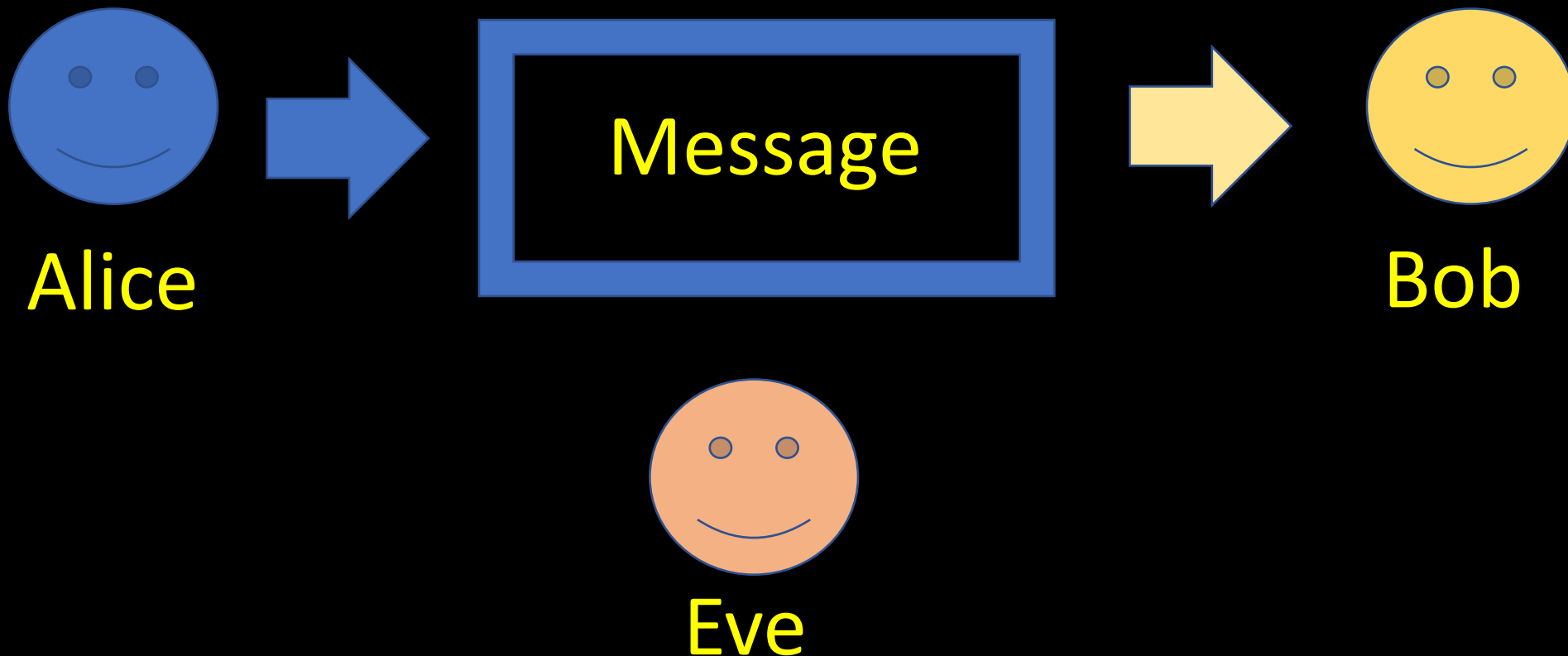
- Message integrity - paired with original value
- Passwords - Do not need original value

Encryption is used to keep data secret

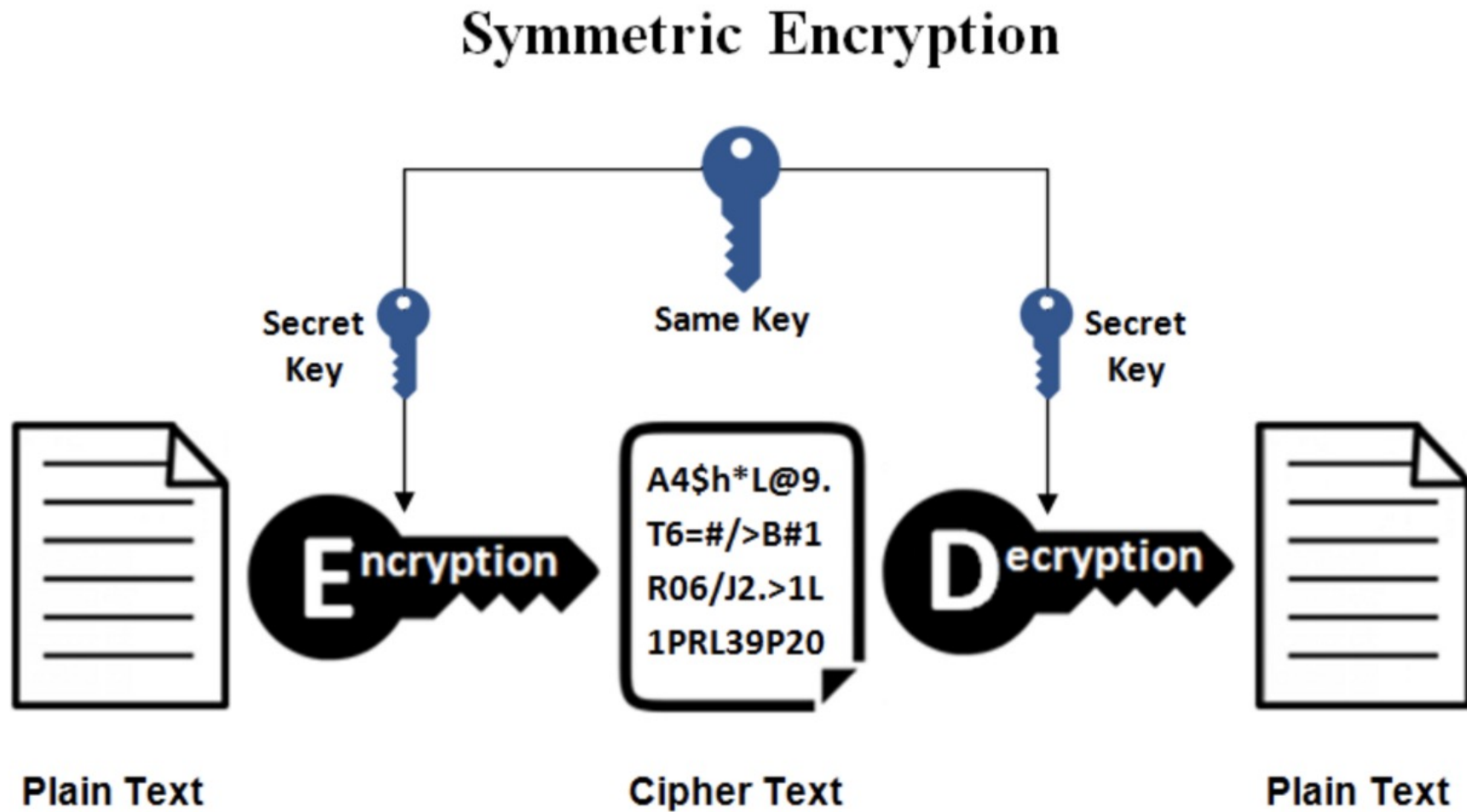
- Keep data safe in transit
- Stored data that is stolen cannot be read

Key Exchange

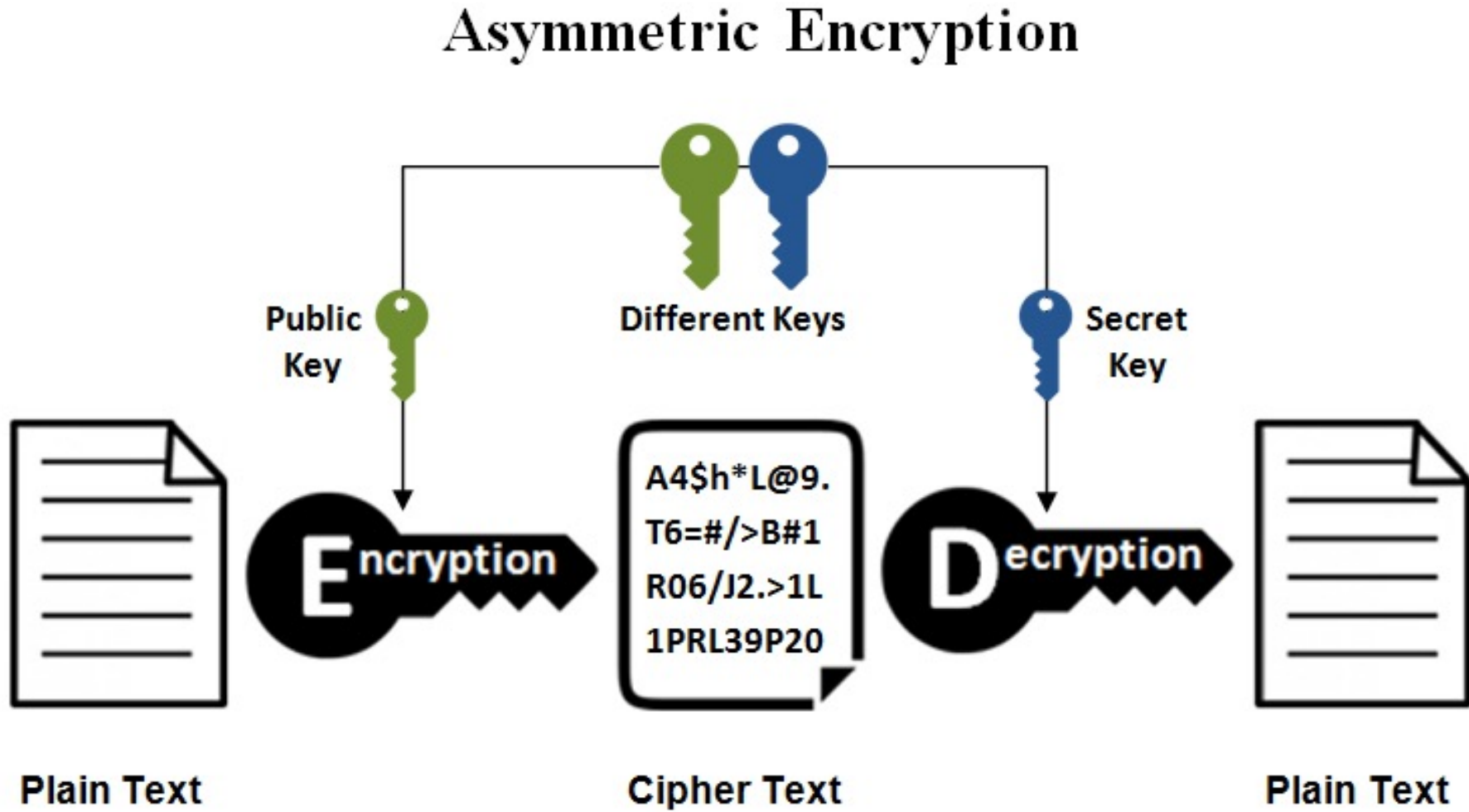
Alice wants to send a super secret message to Bob in a secure channel



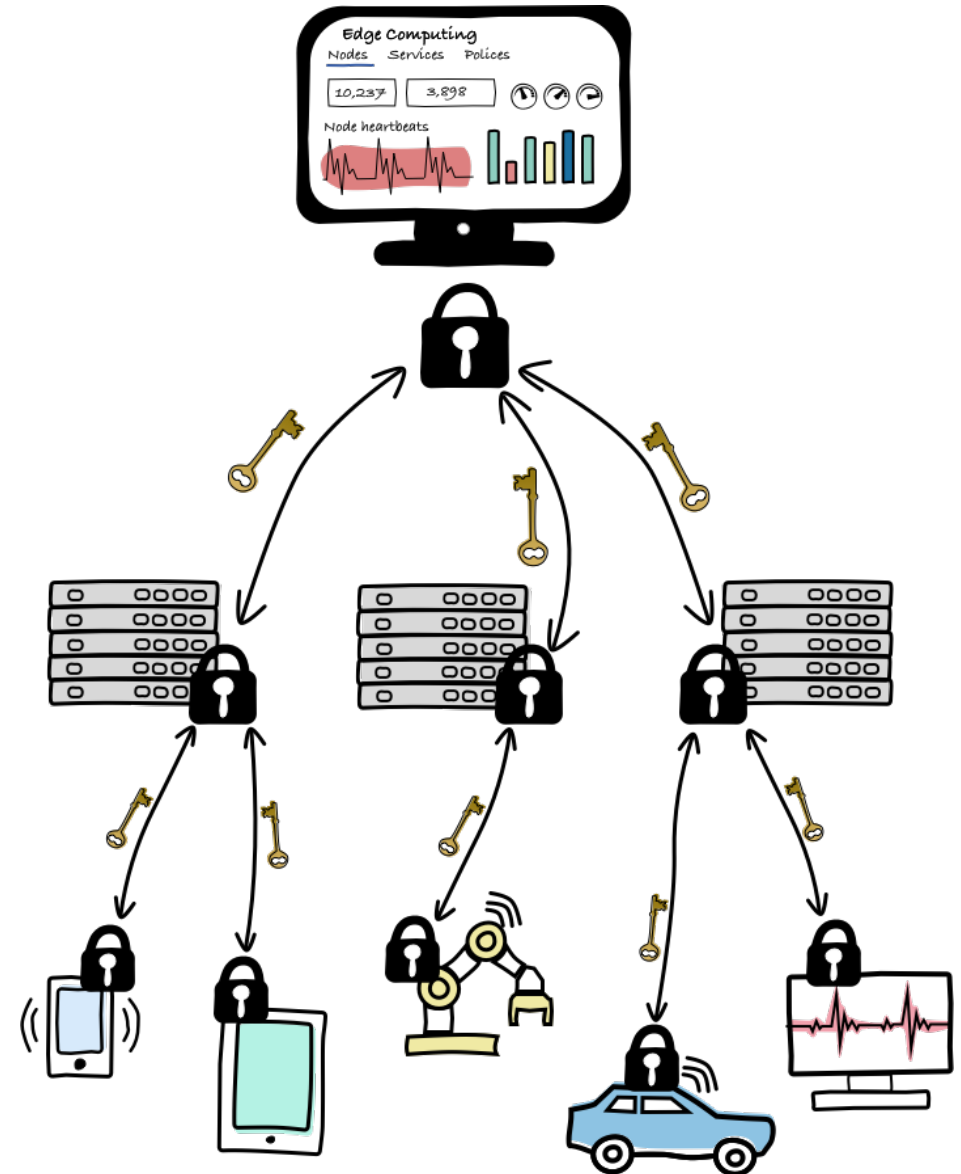
Symmetric encryption



Asymmetric encryption



Edge Computing use case



LAB

<https://medium.com/@rafaelescrich/modern-cryptography-using-go-50e85f0f65af>

<https://medium.com/@ashiqgiga07/asymmetric-cryptography-with-python-5eed86772731>

<https://stackoverflow.com/questions/69643120/rsa-encryption-decryption-between-python-and-golang-not-working>

<https://go.dev/play/p/8WdoyET4599>