

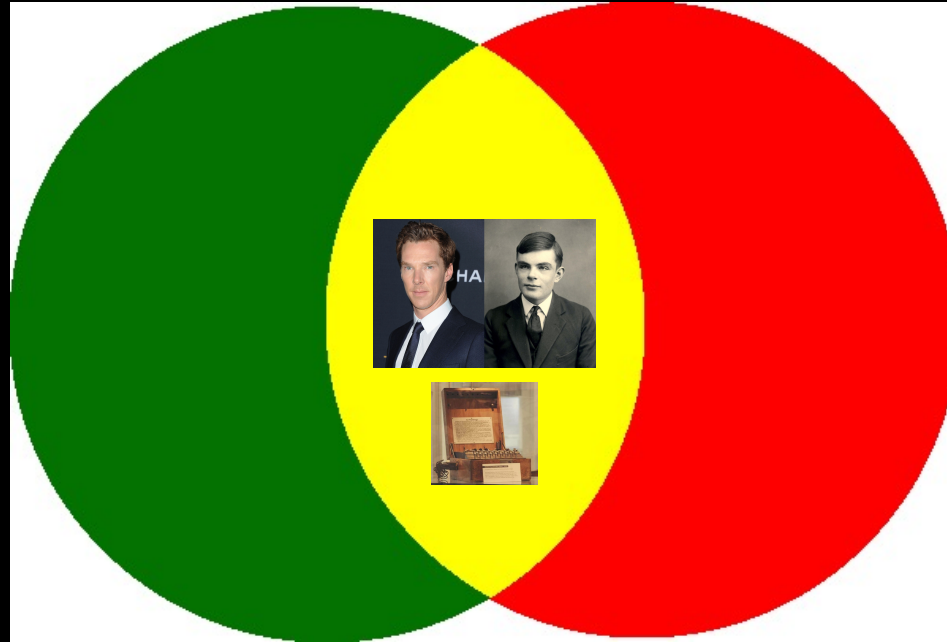
<https://github.com/jiportilla/crypto101>

Cryptography 101  
Hands on lab

- Ivan Portilla
- AI Leader
- [ivanp@us.ibm.com](mailto:ivanp@us.ibm.com)
- 01/23/2022



Artificial  
Intelligence



Cryptography

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

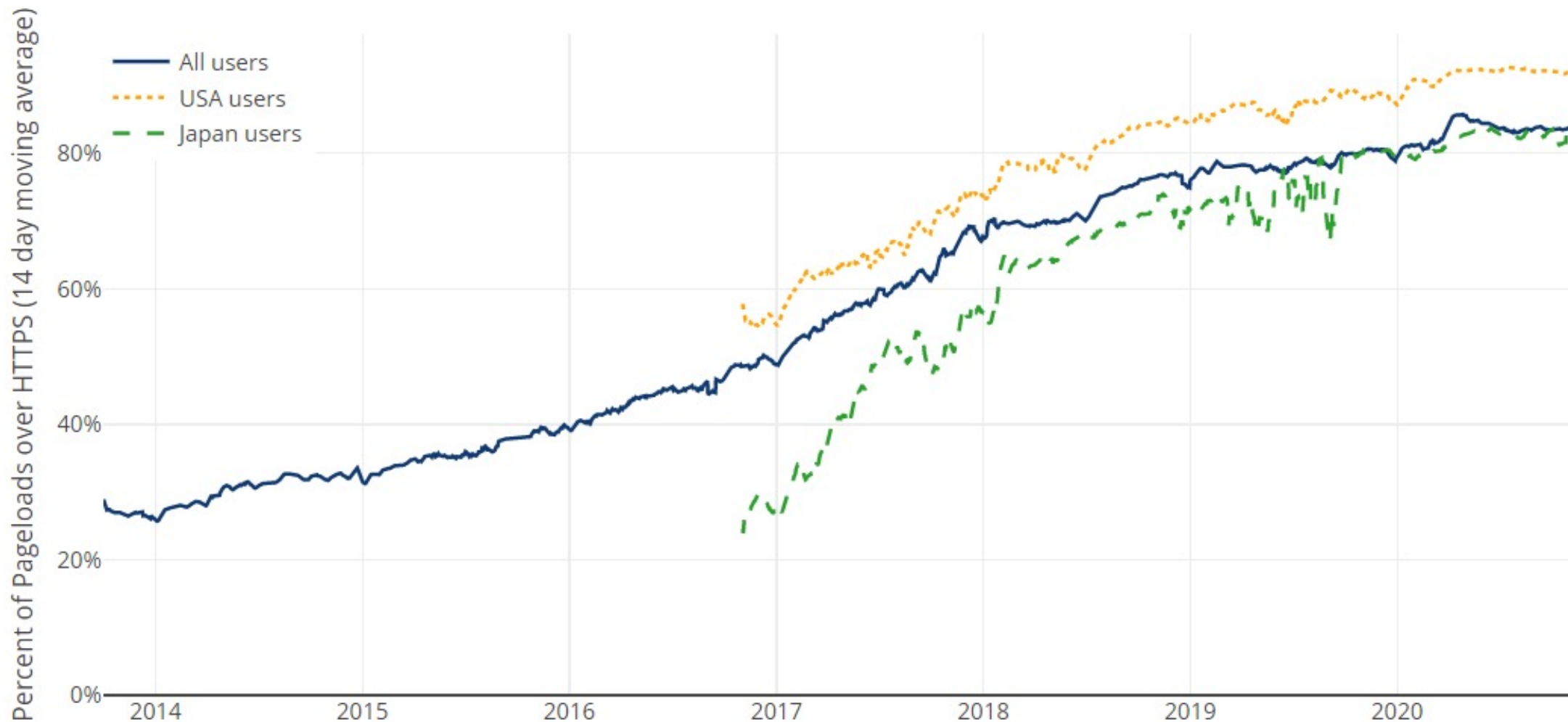
# What is cryptography?

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

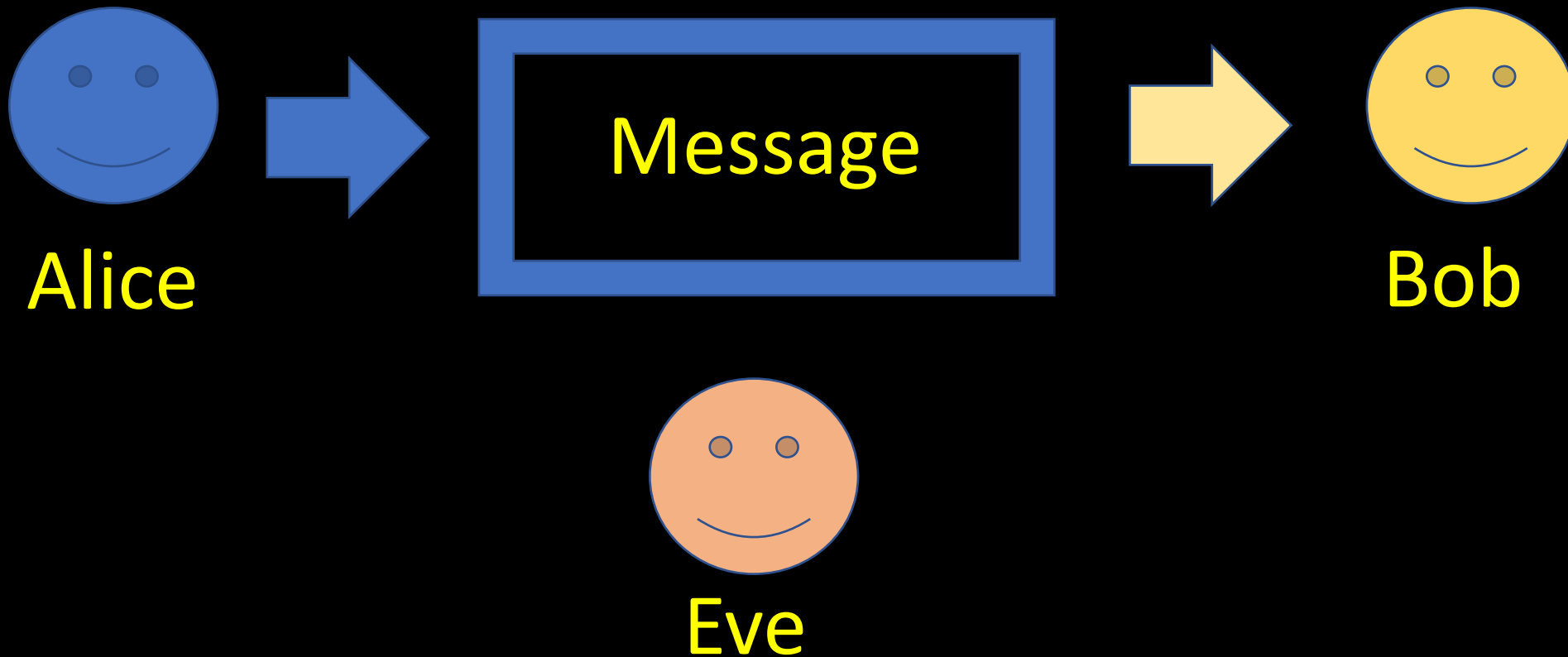
- Message integrity - paired with original value
- Passwords - Do not need original value

**Encryption** is used to keep data secret

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

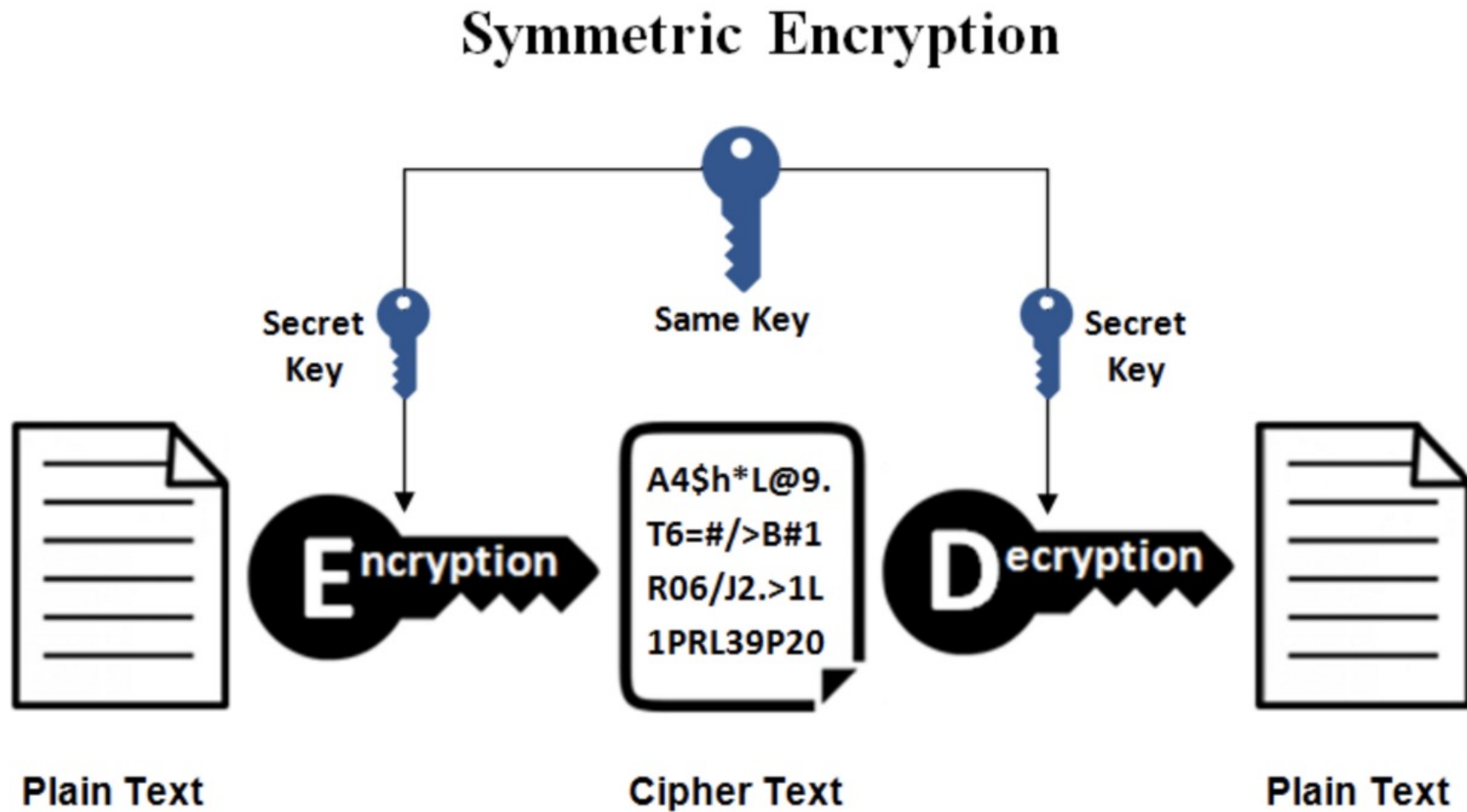
# Key Exchange

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

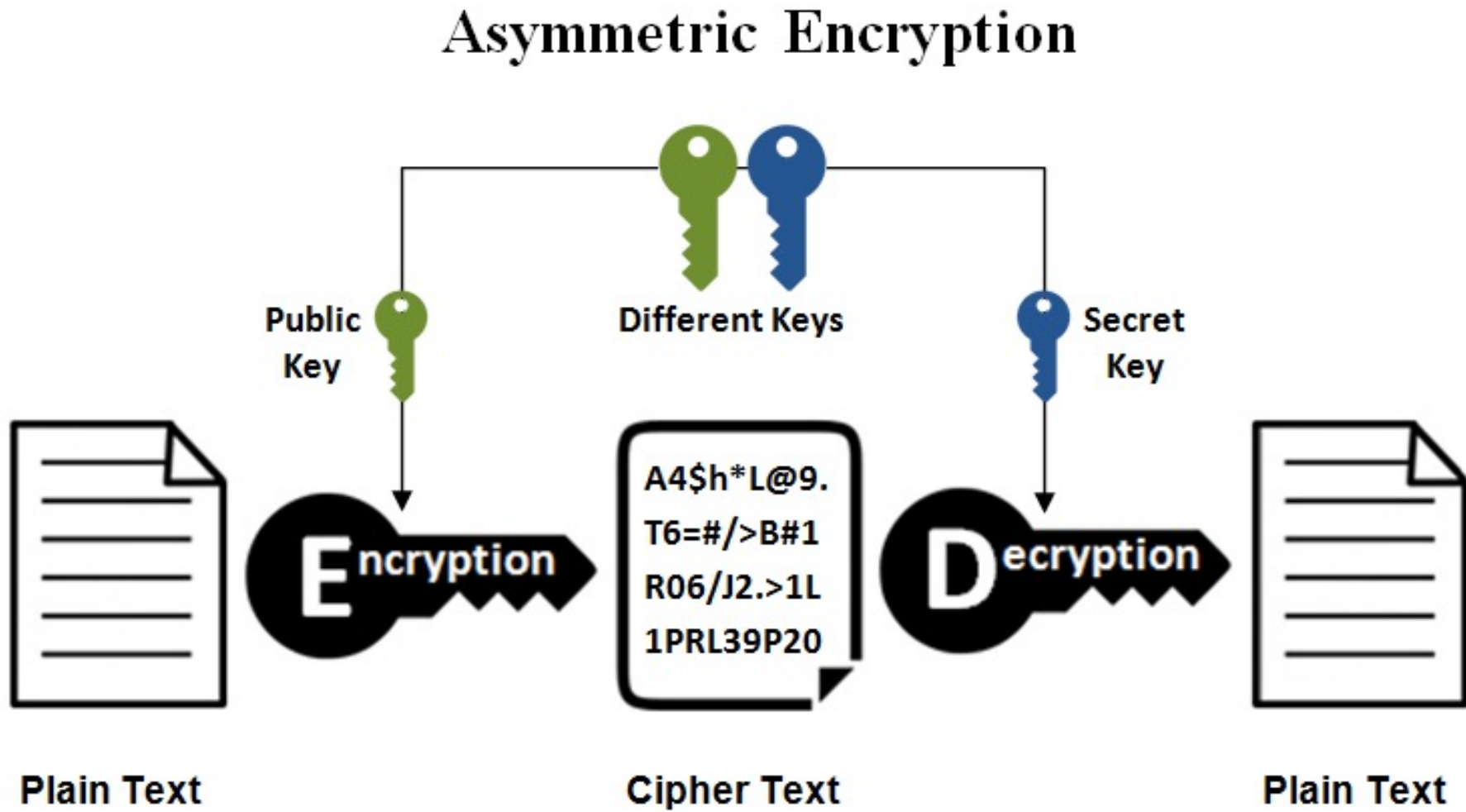




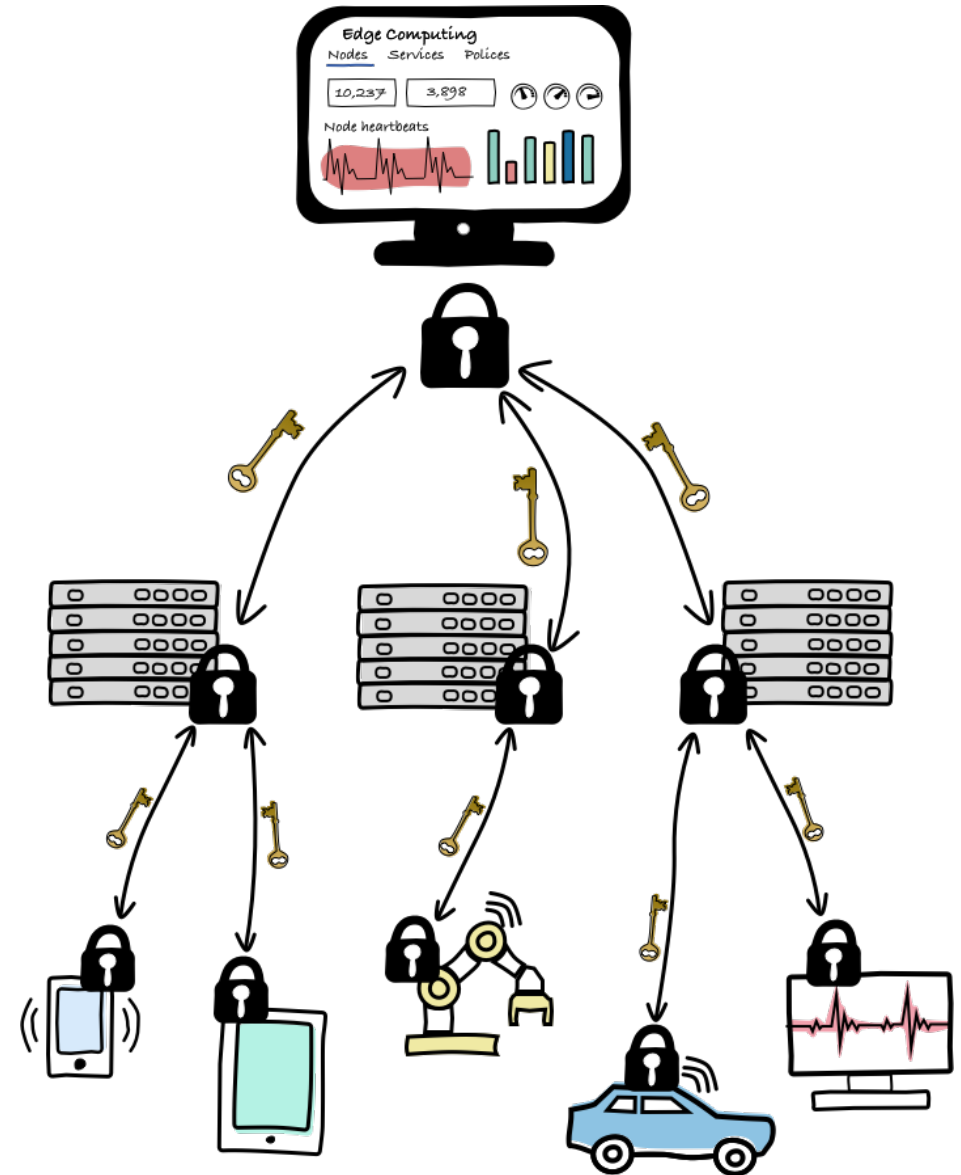
# Symmetric encryption



# 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>