ISOM 5280: PKI

Prof. Weiyin Hong

Department of ISOM, HKUST Business School

Fall 2024

Reading

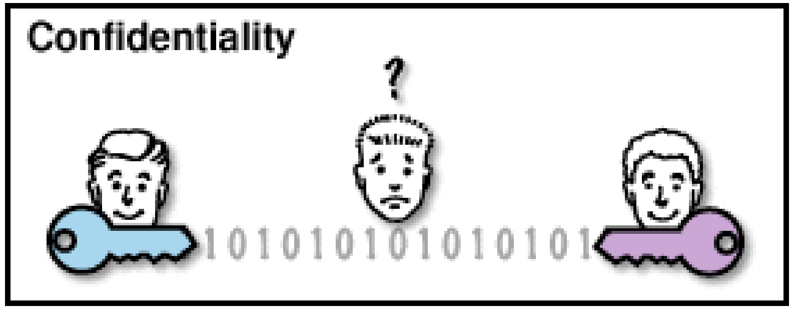
- [WM] Chapter 10

Table of Contents

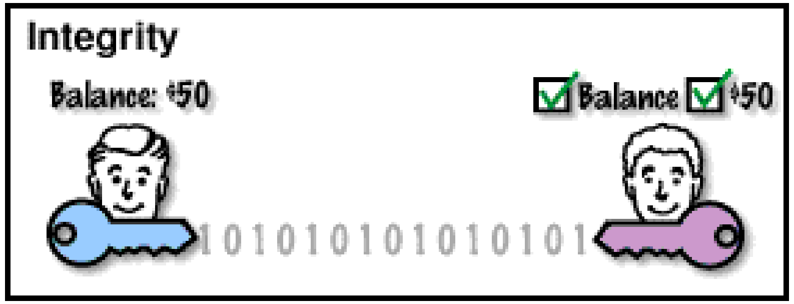
- Symmetric encryption
- Asymmetric encryption - Public Key Infrastructure (PKI)
  - Digital Certificate
- Hybrid system
- Protocols for secure communication
  - SSL/TLS(HTTPS), PGP, WEP/WAP, Bluetooth

Why Cryptography?

- Confidentiality – unauthorized people should not see the message
  - *"Who should see the information?"*

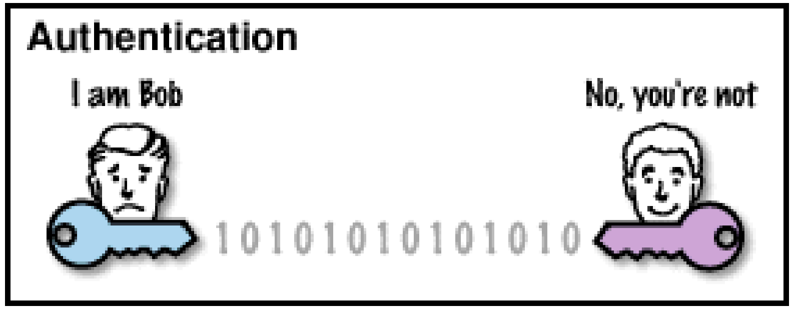


- Integrity – the message is not tampered with during the transmission
  - *"Did anyone change the information?"*

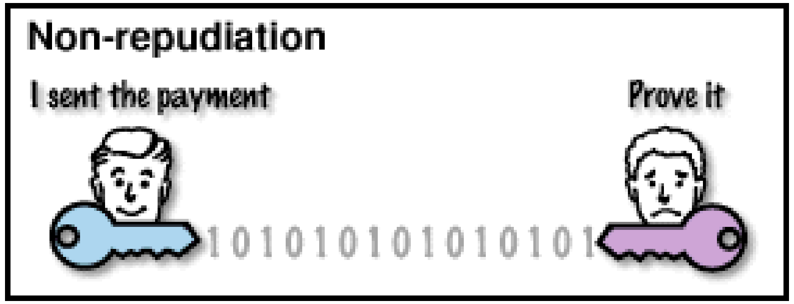


Why Cryptography?

- Authenticity – verify the identity of the person who sent and receive the information
  - *"Who sent and who received the information?"*



- Non-repudiation – prevent someone from denying a transaction
  - *"Can someone deny that he/she had sent a message earlier?"*



Examples in the Conventional World

	√	X
Confidentiality		
Integrity		
Authenticity		
Non-repudiation		

post card
envelope
invisible ink

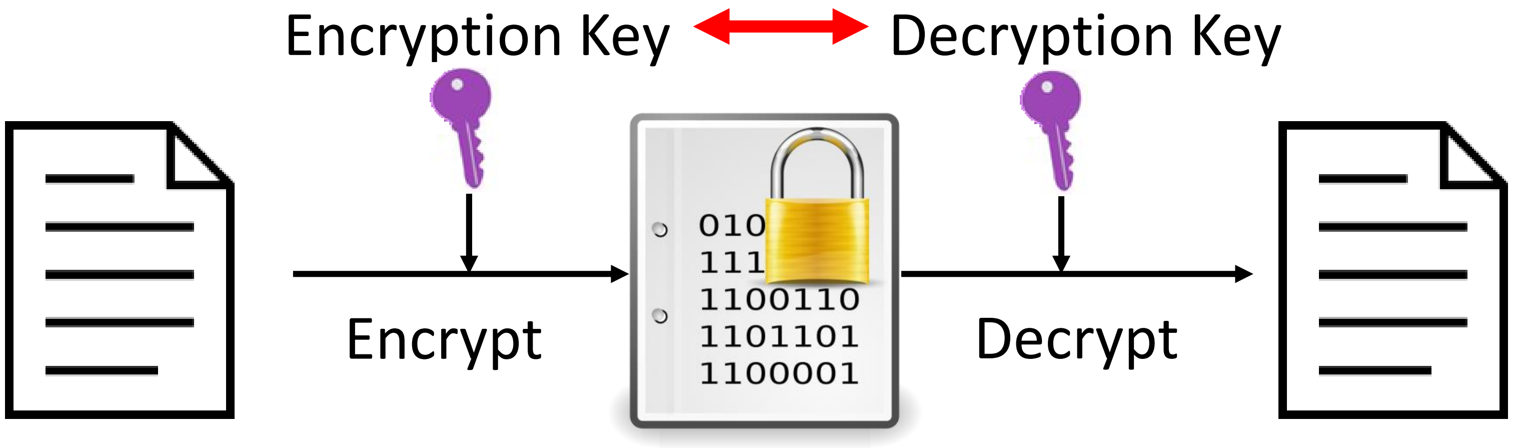
permanent ink
pencil

HKID Card
octopus card
driving license

name
telephone
signature
biometrics
birthday

Symmetric Encryption

- Same key for both encryption and decryption (hence “symmetric” or “secret”)



- Examples – all cipher methods introduced earlier (substitution, transposition, etc.)

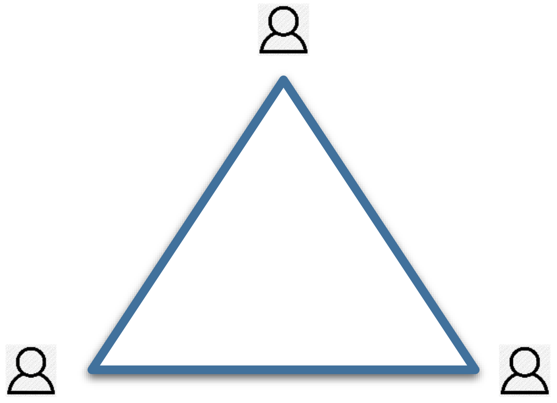
Symmetric Key Implementation

- Data Encryption Standard (DES)
  - Block cipher developed by IBM; endorsed by US government in 1977
  - 56-bit key on 64-bit data block
  - 16 rounds of permutation, character substitution, and XOR operation
  - Brute force attack, in 1998, US$250,000 hardware ⇒ 3 days
- Advanced Encryption Standard (AES)
  - Federal Information Processing Standard (FIPS) cryptographic algorithmic for use within the US government
  - Key lengths of 128, 192, or 256 bits (AES-128, AES-192, and AES-256);
  - 9-13 rounds of operations involving substitution, transposition, XOR, and matrix multiplication
- RC4:
  - A stream cipher with a 40 to 2048-bit key. It generates a keystream by using index.
  - Used in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) with the Hypertext Transfer Protocol over SSL (HTTPS) protocol; and WEP and WPA on wireless networks.
- RC5:
  - It is a block cipher using a 1 to 255 round (12 originally suggested) Feistel-like network with 32, 64, or 128-bit blocks published in 1994. The key size is 0 to 2040 bits. Also uses modular addition and bitwise XOR.

Symmetric Key Cryptosystem

- No. of keys needed with n parties

$$ {}_nC_2 = n(n-1)/2 $$



- Advantage:
  - Fast operation
  - Simple
  - Theoretically strong if key is secure
- Disadvantage:
  - Key distribution and management
  - Fast operation ⇒ easier to break

- What if the key is lost?
- The security will break down.

Cryptographic Algorithm

- Symmetric encryption: requires the same secret key to encipher and decipher the message.

Private-key Pairs

- Asymmetric encryption: Use two different but related keys: a private key and a public key. Either key can be used to encrypt a message, but then the other key is required to decrypt it.

Public & Private Keypair

Asymmetric Key Systems

- A key pair for each person
  - One as a public key – open for public access
  - The other as private key – restricted to owner
  - **Deriving the private key from the public key alone is not possible!**

Public Key Cryptosystem

- Foundation: mathematics!
  - Factoring a product of two large prime numbers is extremely challenging

-----BEGIN PGP PRIVATE KEY BLOCK-----

[illegible]

-----END PGP PRIVATE KEY BLOCK-----

→ Easy

$$123 \times 731 = 89{,}913$$

← Difficult!

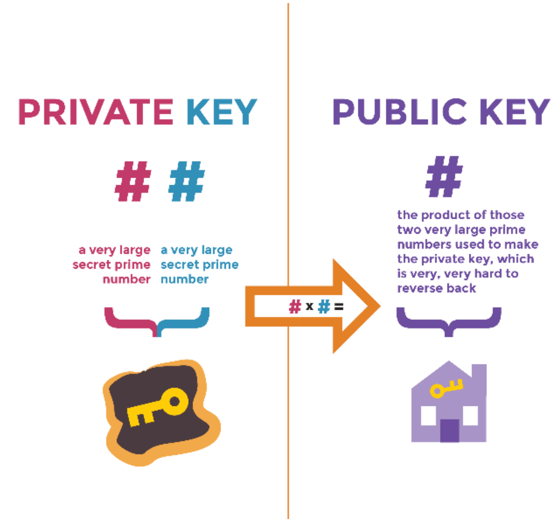

PRIVATE KEY
# #
a very large secret prime number
a very large secret prime number
# x # =
PUBLIC KEY
#
the product of those two very large prime numbers used to make the private key, which is very, very hard to reverse back

Image source: SSD.EFF.ORG

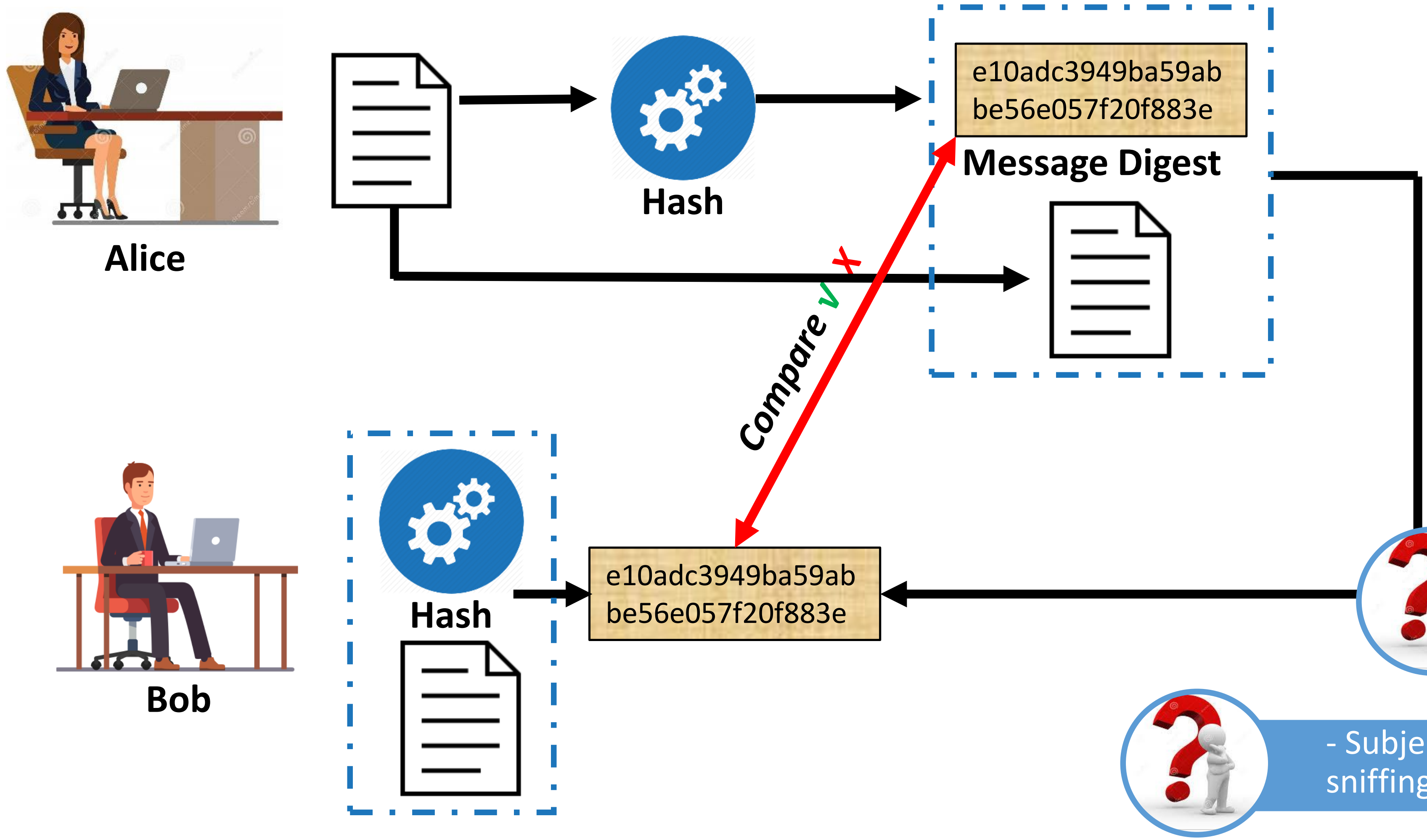
Group Challenge

- Can your team demo how this may work in practice for message exchange between two person?

Public Key Infrastructure (PKI)

- Benefits:
  - Easier key management and distribution
  - The private key is never distributed and therefore is more secure
  - Scalable
- Weakness:
  - Slow to generate fresh strong keys
  - Slow to encrypt
- Common public key systems
  - RSA (Rivest–Shamir–Adleman) [proposed in 1977]
  - There are no published methods to defeat the system if a large enough key is used.

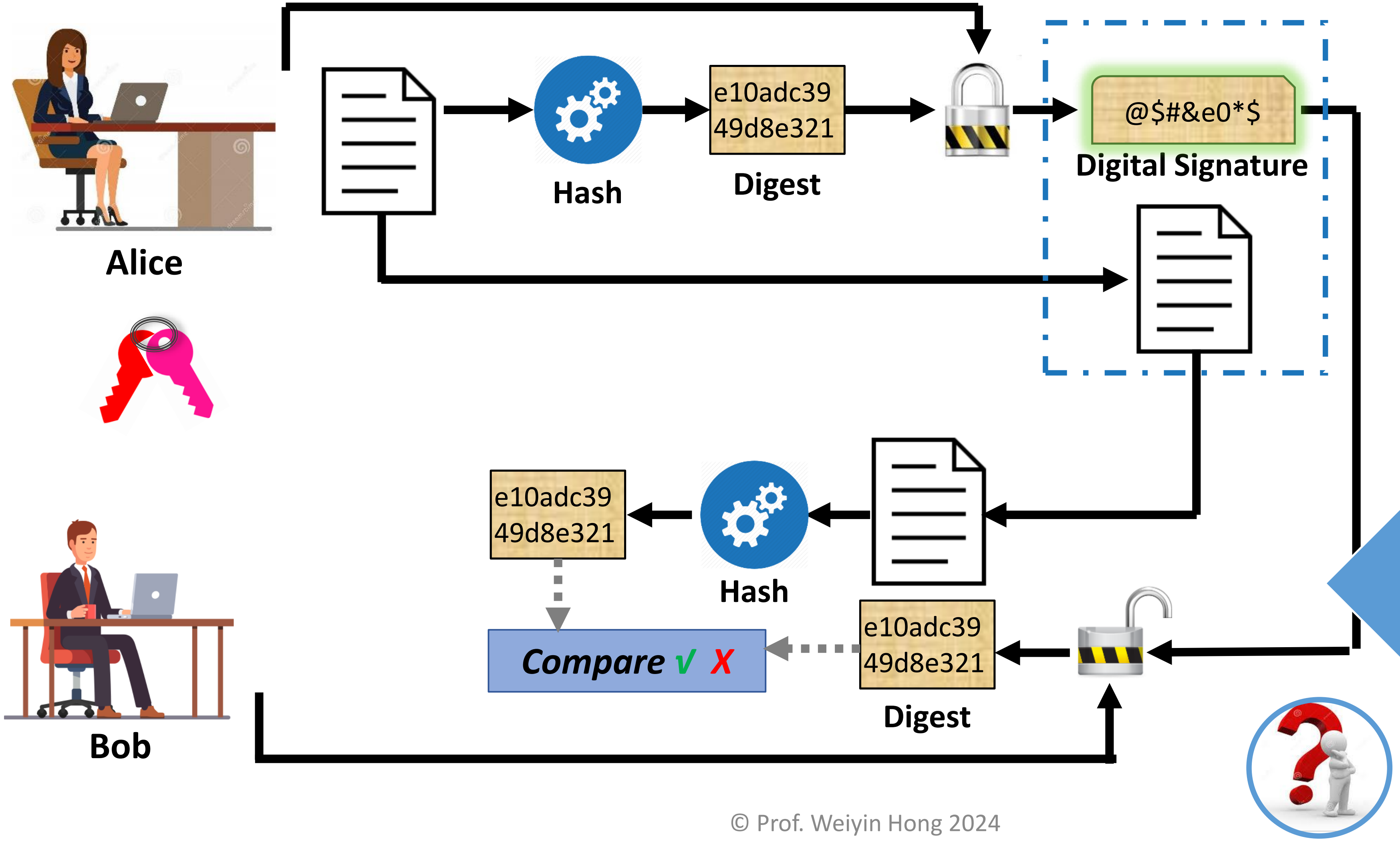
Revisit: Hash as Message Digest



- Does this process ensure confidentiality and integrity? – only integrity

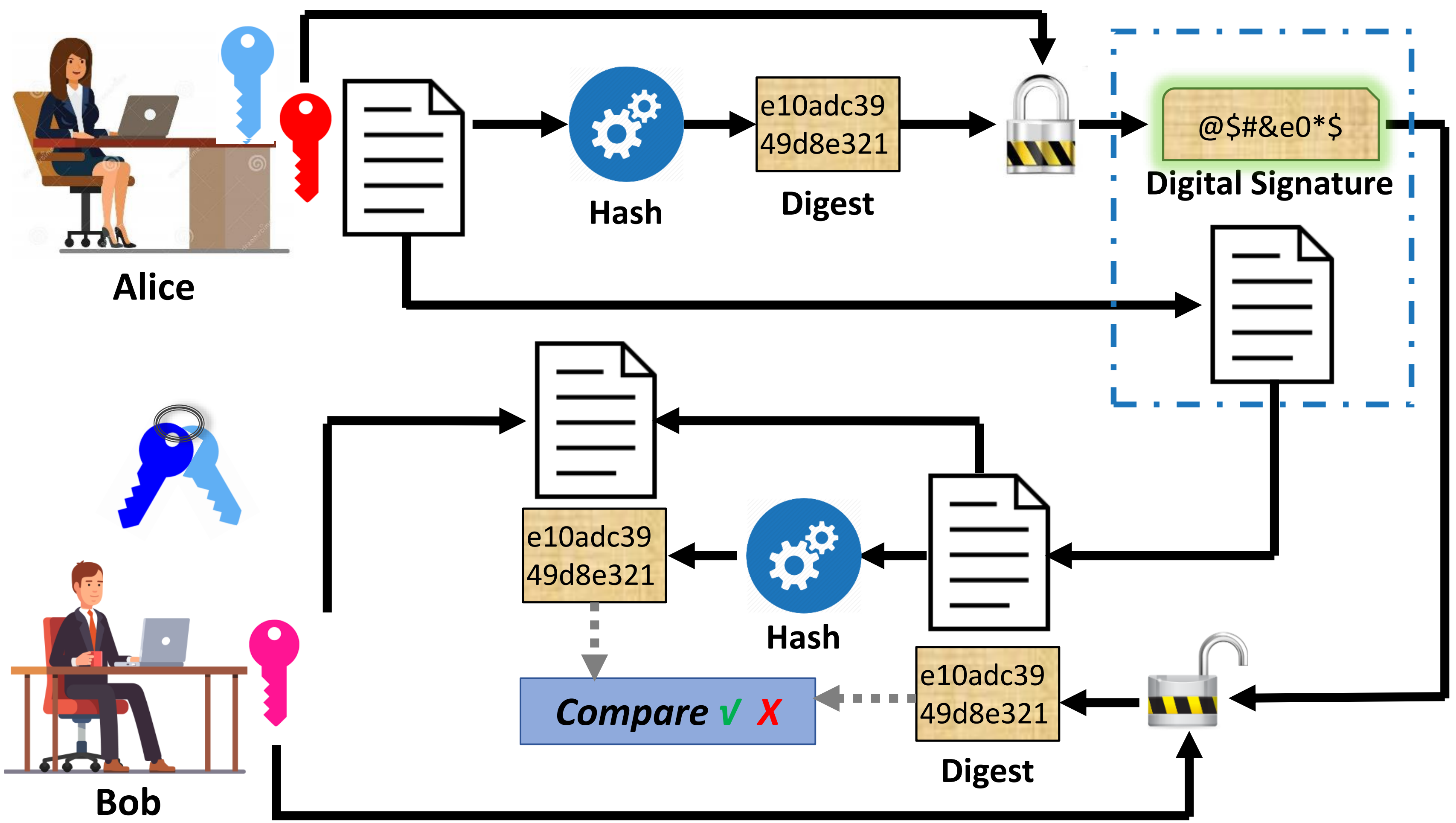
- Subject to what types of attack? – sniffing, spoofing, and man in the middle

Digital Signature of Sender



- Does this process now ensure confidentiality, integrity, and authenticity?
- Only ensures integrity and authenticity of the sender.

PKI with Digital Signature

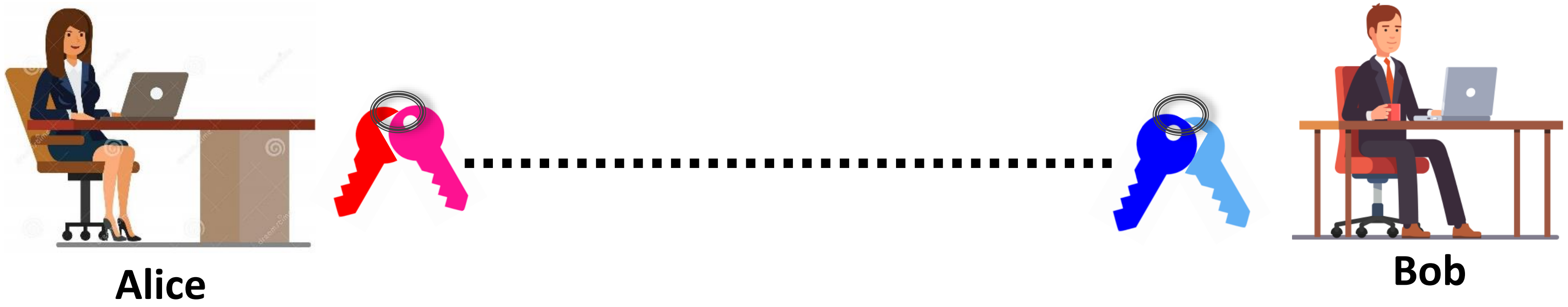


Digital Certificate

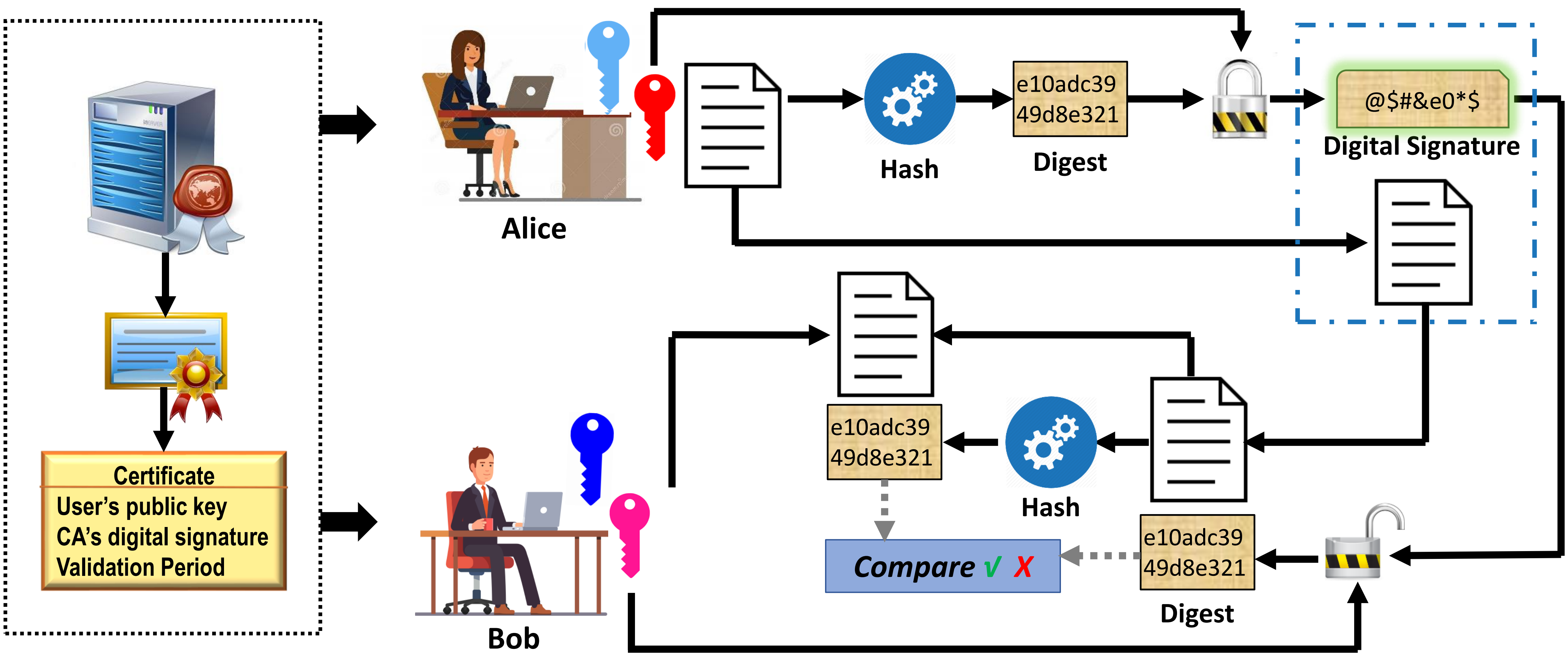
- How to ensure the validity of someone's public key?

- A digital certificate is an electronic document that contains a public key value and identifying information about the entity that controls the key.
- Often issued by a third party, i.e., a certificate authority (CA).

Certificate Authority



PKI with Digital Certificate



In-Class Try Out (1)

- Download an installation file
- Right click for its properties
- Go to the “Digital Signatures” tab (does all program have this tab?)
- Click on the signature, and click “Details”

In-Class Try Out (2)

1. Open Chrome and visit www.amazon.com
2. Click on the Secure logo before https://
3. Click on “Connection is secure”
4. Click on “Certificate is valid” and check both the “General” and “Details” tabs
5. Answer the following questions:
    1) Which CA issued this digital certificate?
    2) Who is the root CA for this certificate?
    3) What’s the validation period of this certificate?
    4) What is the subject’s public key?
    5) What hash function is used to generate a digital signature of the certificate?
6. You may try another popular website’s digital certificate.

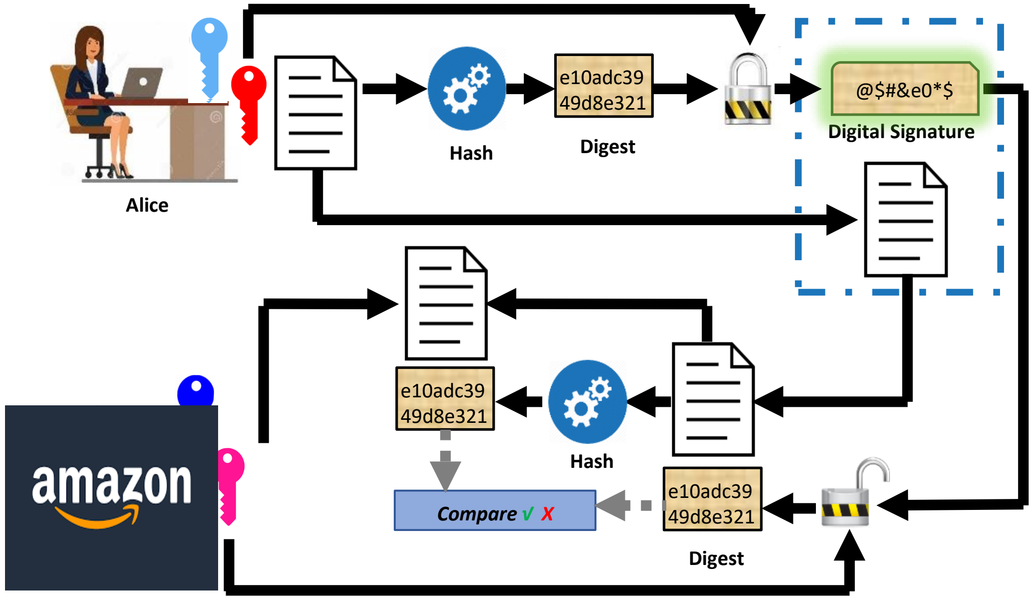
In-Class Try Out (3)

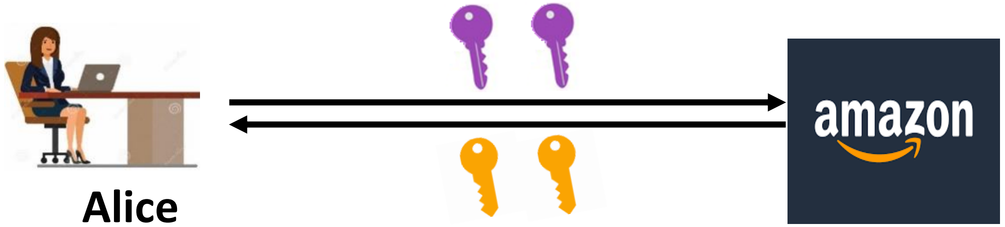
- Open Google Chrome Settings
- Click “Privacy and Security”
- Click “Security”
- Scroll down and click “Manage certificates”
- Click on “Chrome Root Store” on the left menu
- Double click on any certificate to check it out.

Hybrid Cryptography System

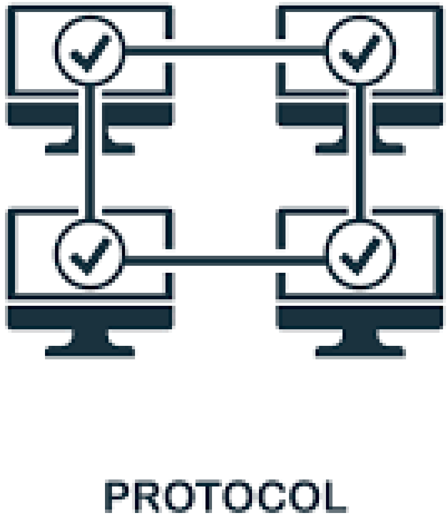
- Asymmetric key algorithm is used to verify the identity of the owner and its public key.

- Once connection is built, symmetric key (session key) is used to encrypt and decrypt all following traffic between the two parties.



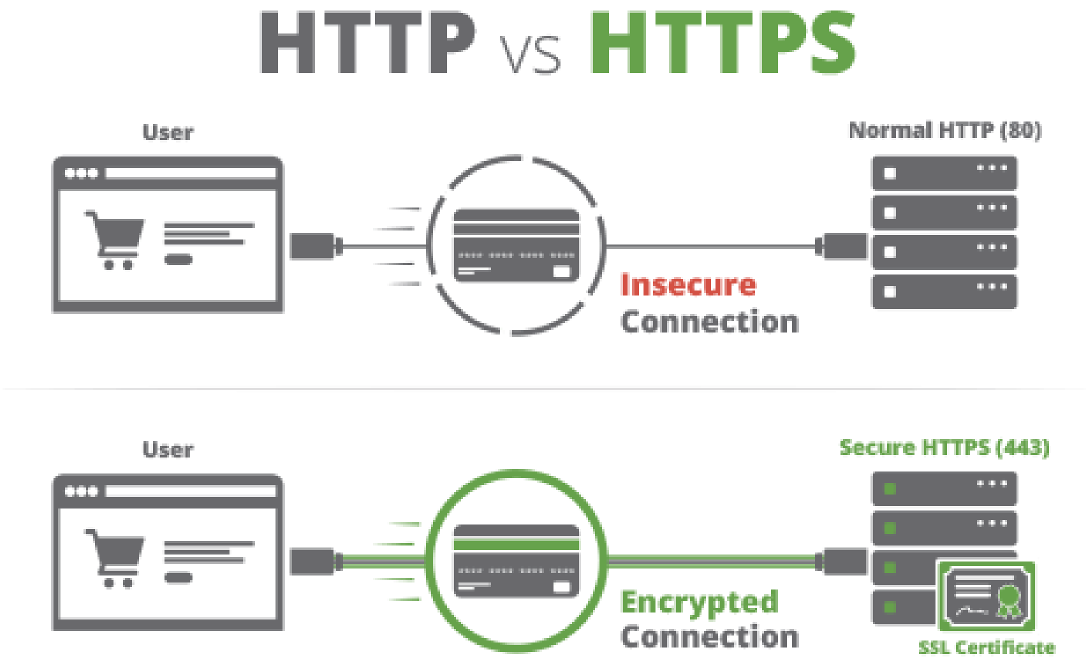


Protocols for Secure Communication

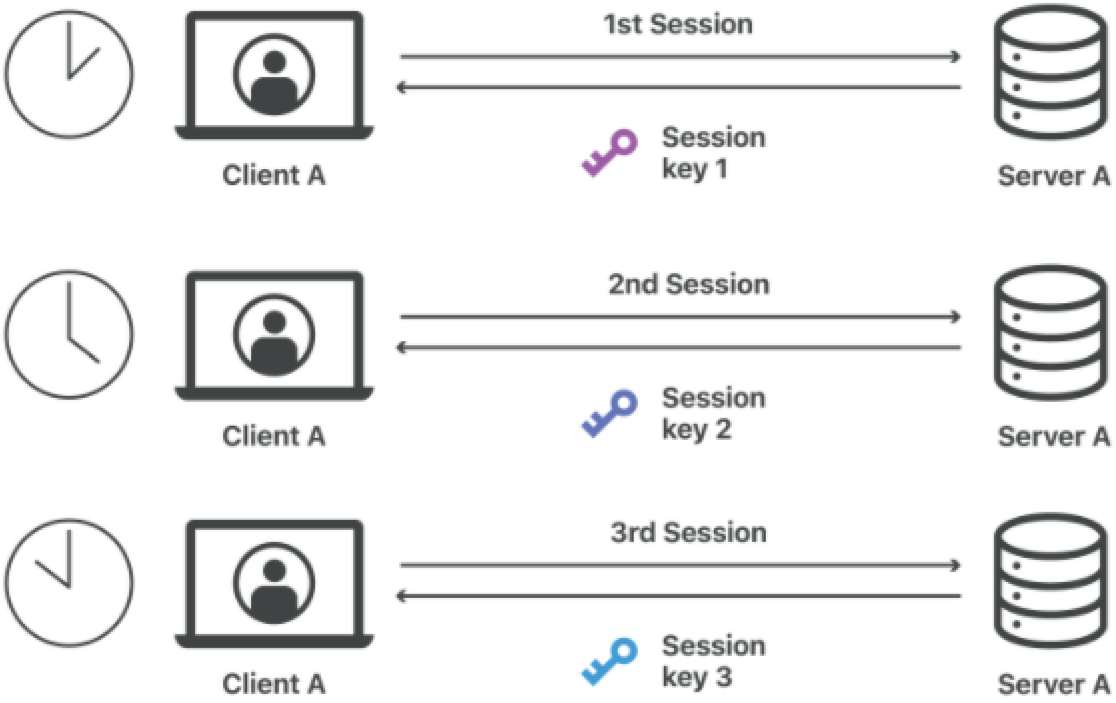


Environment	Protocols
Web (https://)	SSL, TLS
Email	S/MIME, PEM, PGP
Wireless	WEP, WPA, WPA2, WPA3
Bluetooth	Passkey only

HTTP vs. HTTPS



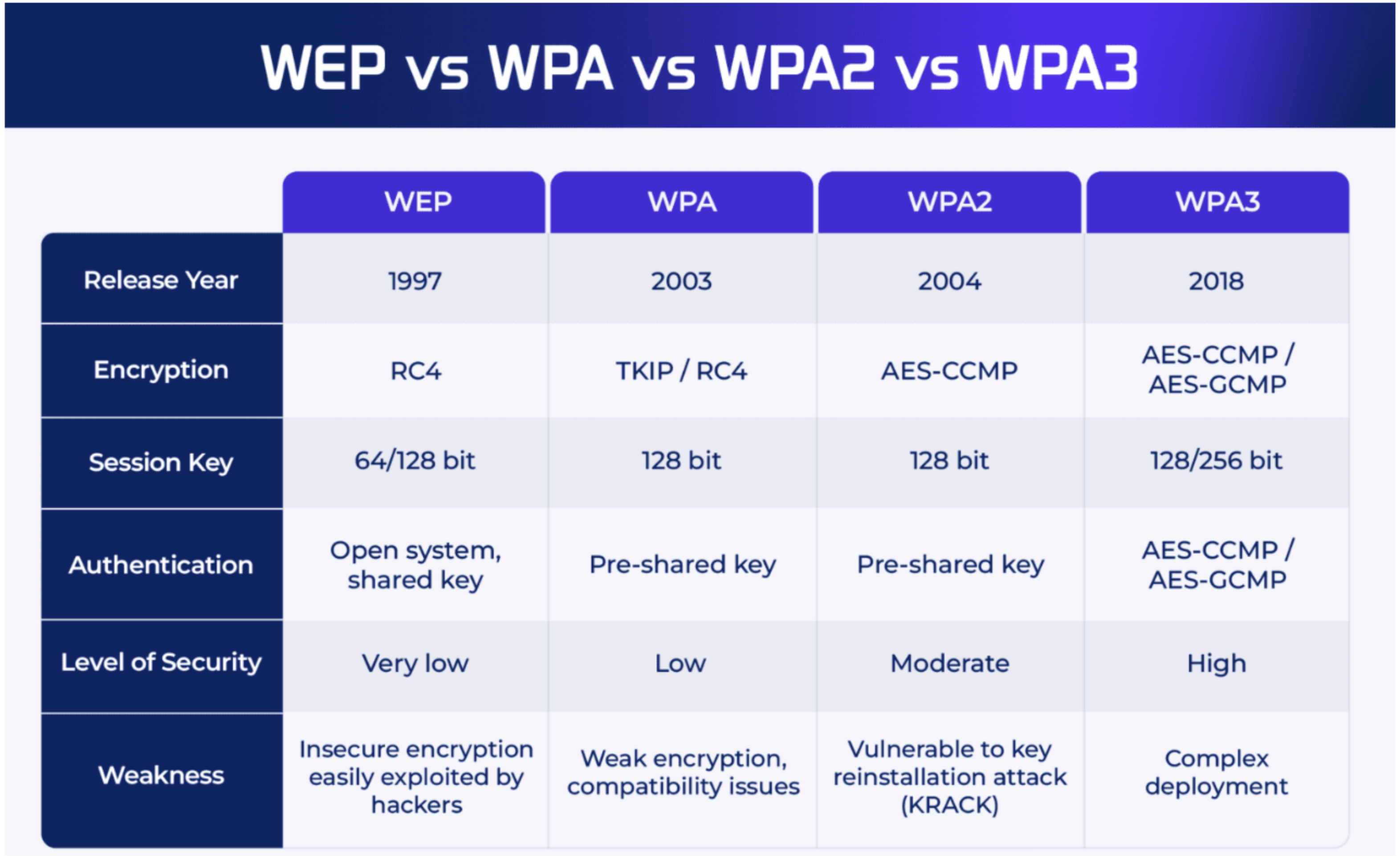
SSL (Secure Socket Layer)



PGP

- Pretty Good Privacy (PGP) is a hybrid cryptosystem, available free or at low cost.
- Becomes the open-source standard for encryption and authentication of email and file storage applications.
- PGP uses ZIP to compress the message after it has been digitally signed, but before it is encrypted.

WEP vs. WAP



WEP vs WPA vs WPA2 vs WPA3

	WEP	WPA	WPA2	WPA3
Release Year	1997	2003	2004	2018
Encryption	RC4	TKIP / RC4	AES-CCMP	AES-CCMP / AES-GCMP
Session Key	64/128 bit	128 bit	128 bit	128/256 bit
Authentication	Open system, shared key	Pre-shared key	Pre-shared key	AES-CCMP / AES-GCMP
Level of Security	Very low	Low	Moderate	High
Weakness	Insecure encryption easily exploited by hackers	Weak encryption, compatibility issues	Vulnerable to key reinstallation attack (KRACK)	Complex deployment

Bluetooth

- Can be exploited by anyone with a range of approximately 30 feet (10 meters)
- Do not accept an incoming communications pairing request unless you know the identity of the requester.
- Avoid setting up pairing in public
- Delete unused bluetooth connections
- Disable bluetooth when not in use