TRANSPORT LAYER SECURITY (TLS)

The Backbone of Secure Communication

Presented By:
Md. Ibrahim
Saad Al Athar Chowdhury
Md. Sajid Islam

Introduction to TLS

What is TLS?

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network, such as the Internet. TLS replaced SSL in 1999.

Key Features:

- Encryption:
    - Ensures that the data transferred between users and servers is unreadable to attackers.
- Integrity Verification:
    - Guarantees that data has not been altered during transit.
- Authentication:
    - Confirms the identity of the server and optionally the client.

Why TLS Matters

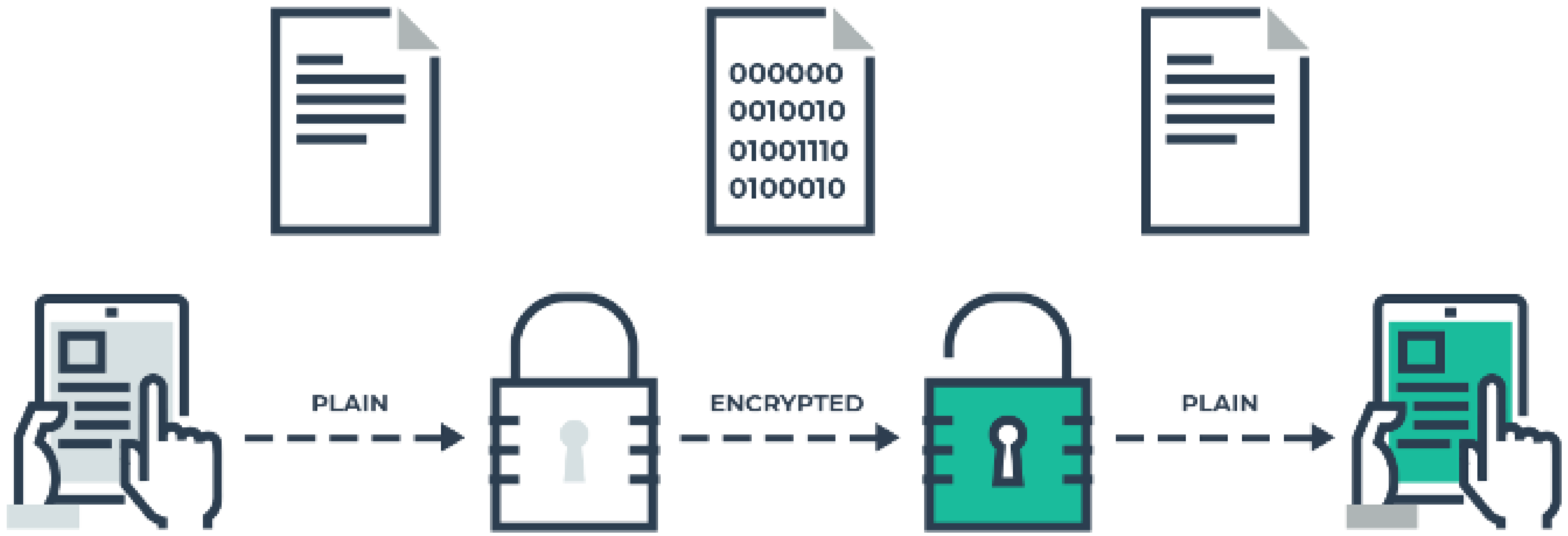
Importance

- Protects sensitive information like passwords and financial data.
- Essential for secure online interactions, including e-commerce, banking, and email.

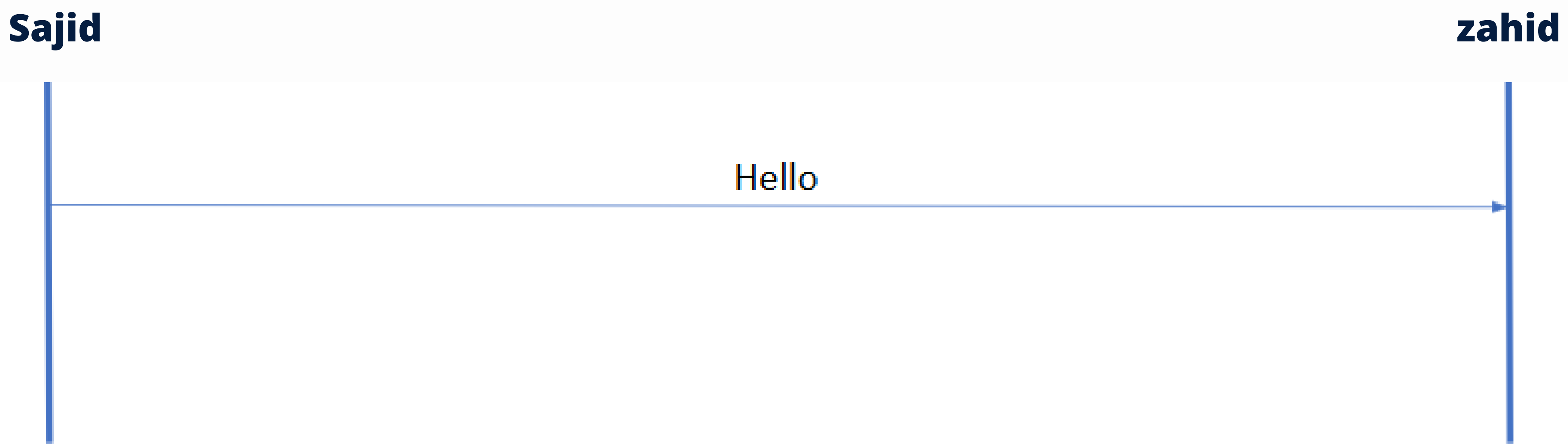
Prevention

- Shields against:
  - Eavesdropping: Blocks unauthorized listening.
  - Tampering: Maintains data integrity.
  - MITM Attacks: Prevents interception by attackers.

What is Cryptography?



Sajid want to communicate with Zahid



Sajid

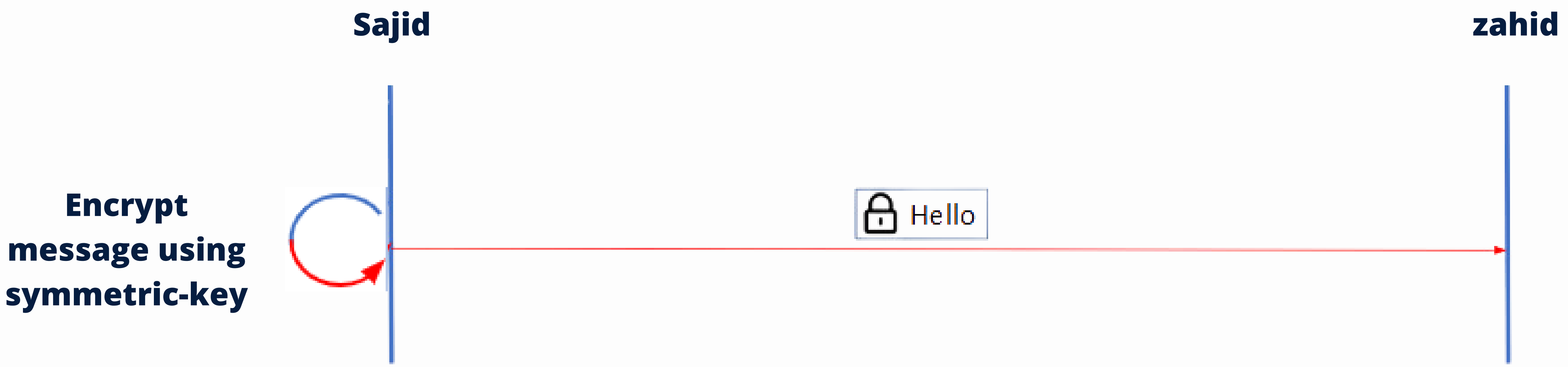
zahid

Hello

Plain
Text

Sajid want to communicate with Zahid

Symmetric Key Encryption



How to exchange key securely?

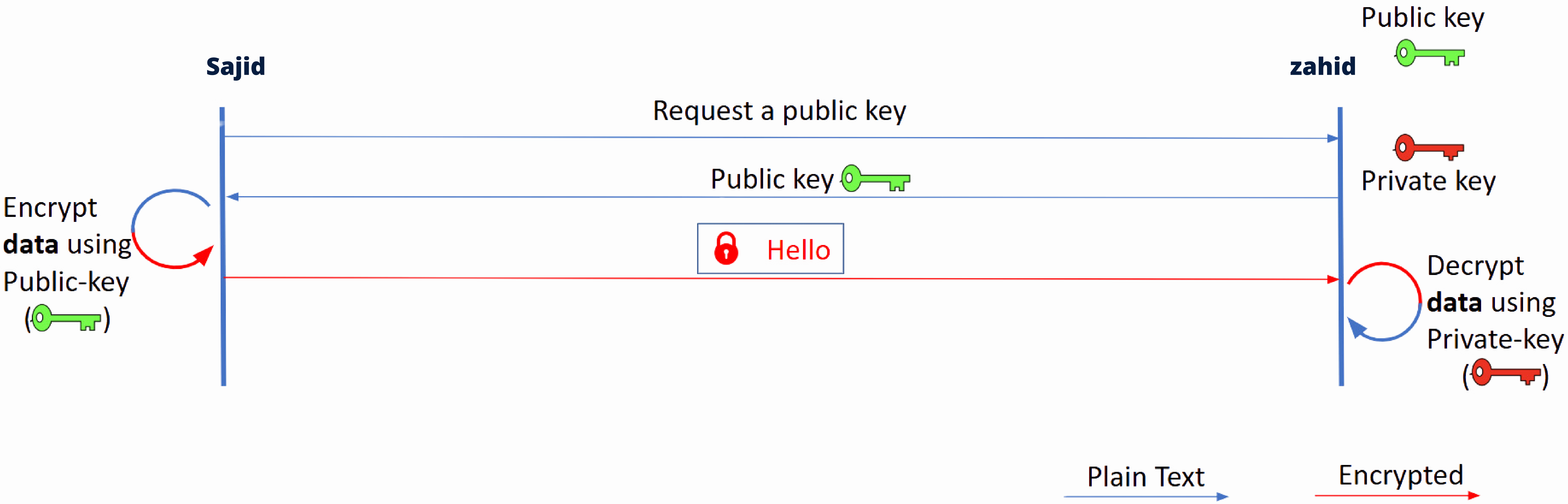
How to exchange key securely?

Asymmetric Key Encryption.

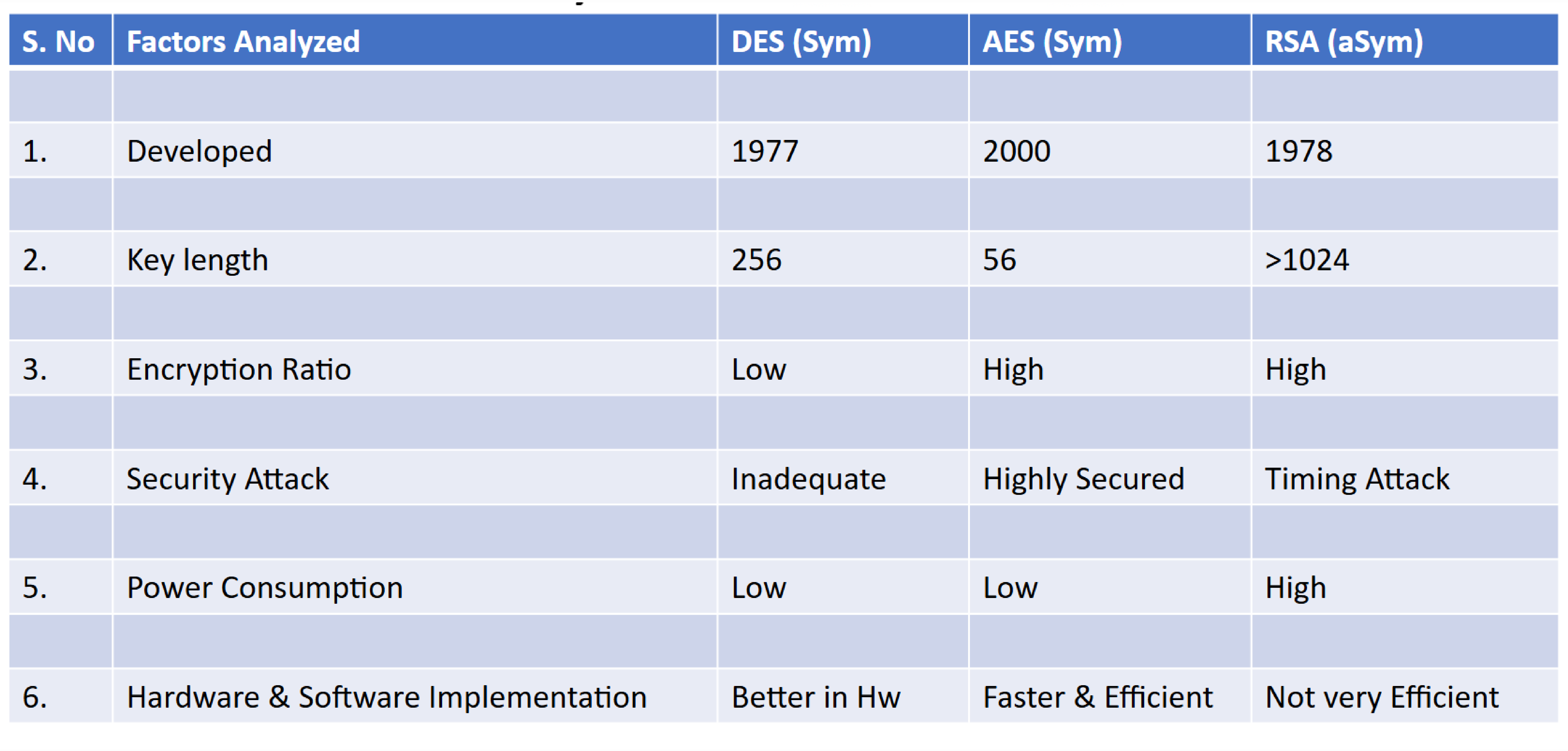
Key 1
(Binary Number)

Key 2
(Binary Number)

Public Key Encryption (Asymmetric cryptography)

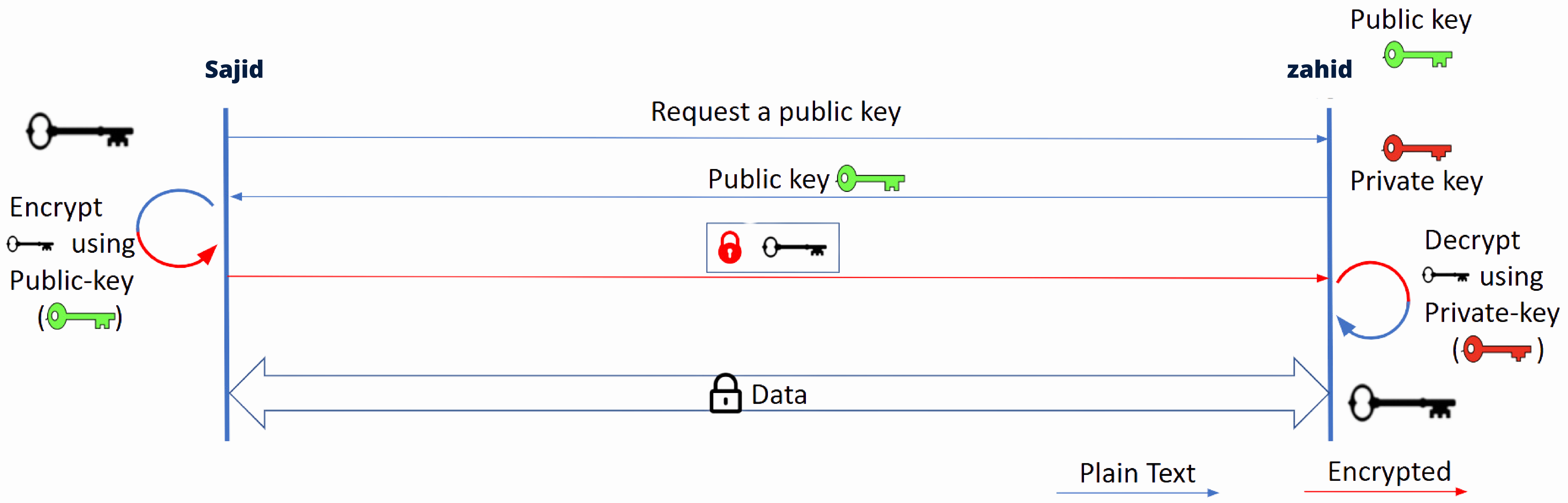


Performance Analysis

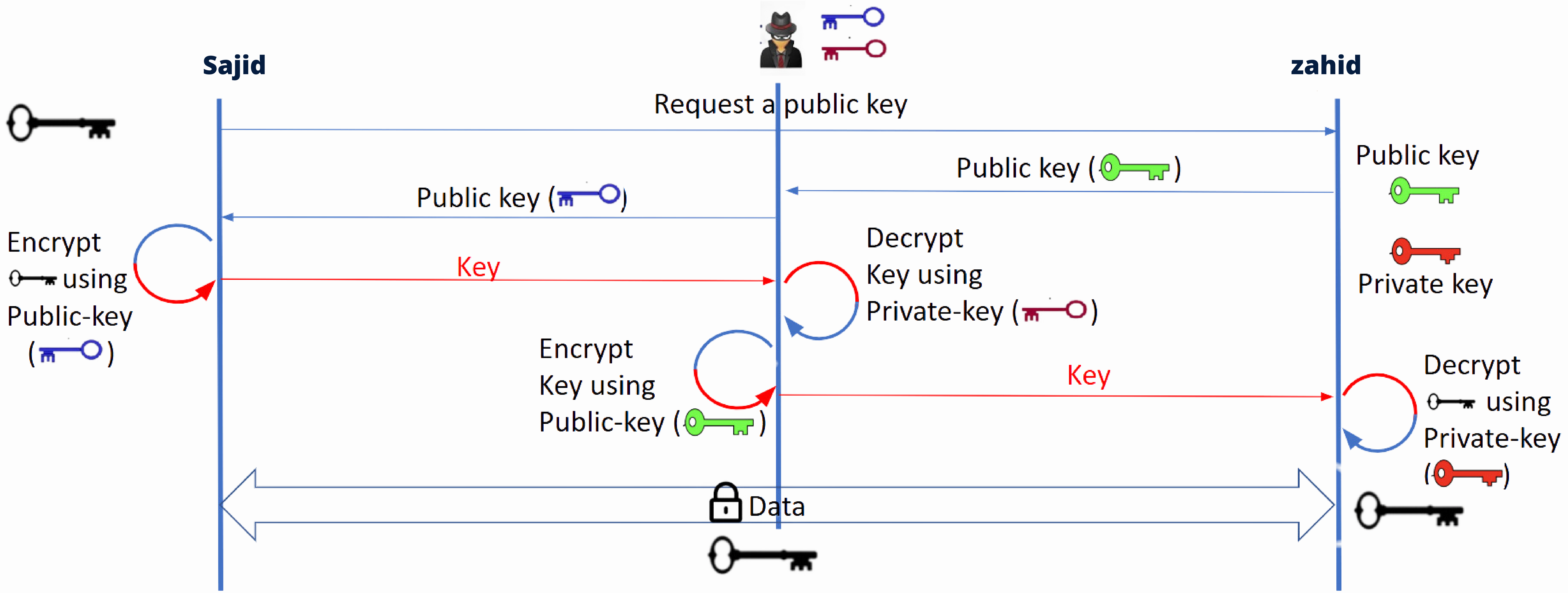


S. No	Factors Analyzed	DES (Sym)	AES (Sym)	RSA (aSym)
1.	Developed	1977	2000	1978
2.	Key length	256	56	>1024
3.	Encryption Ratio	Low	High	High
4.	Security Attack	Inadequate	Highly Secured	Timing Attack
5.	Power Consumption	Low	Low	High
6.	Hardware & Software Implementation	Better in Hw	Faster & Efficient	Not very Efficient

Hybrid Solution



What is the issue with above solution?



Even though encrypted channel established but crypto key known to MITM. So communication is no more secure

How to prevent Man In The Middle(MITM) attack?

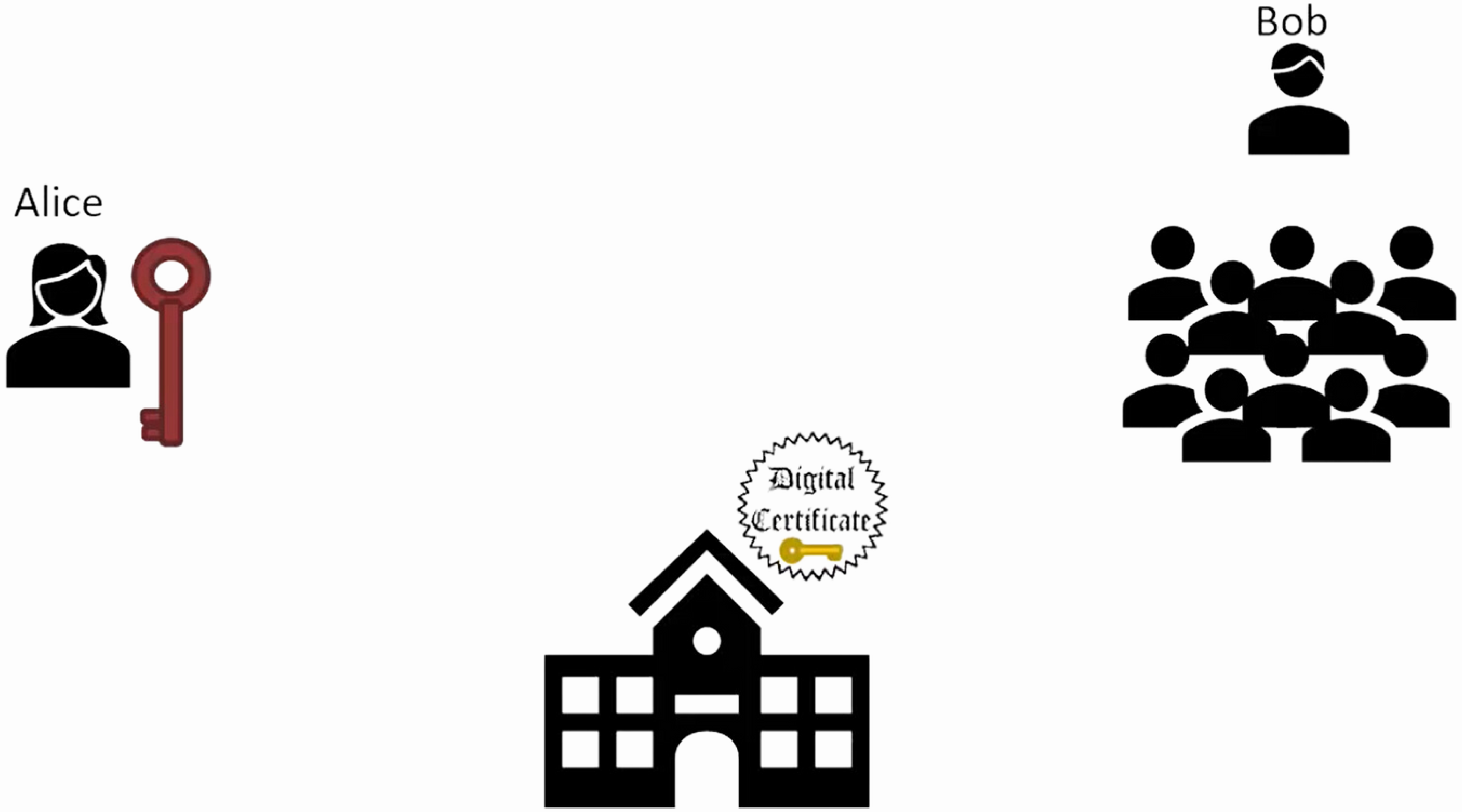
Identity Management

Digital Certificate

Certificate Authority

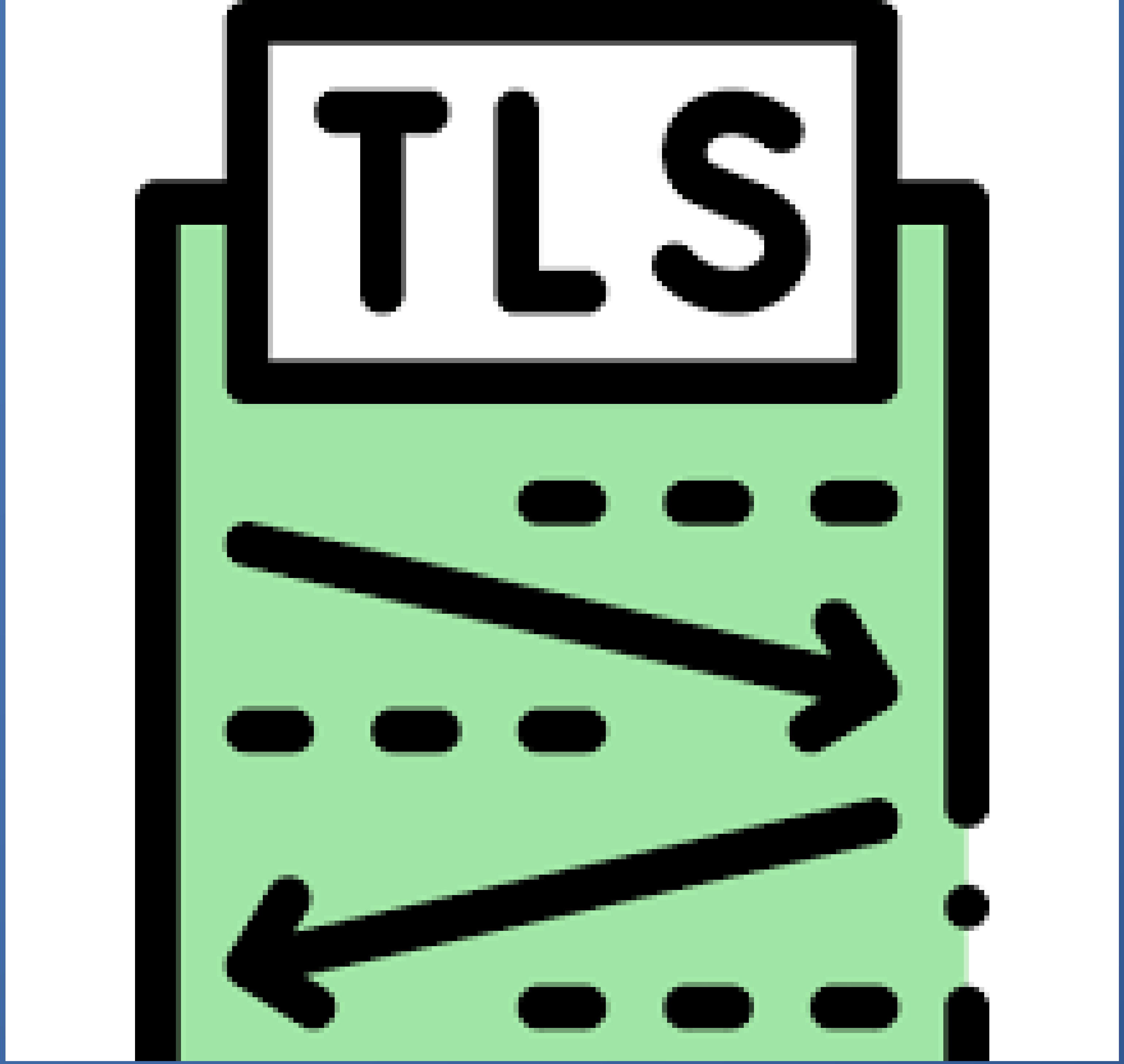
- Generate, issue, and distribute public key certificates
- Distribute CA certificates
- Generate and publish certificate status information
- Revoke public key certificates

Verifying



Bob

Alice



HOW TLS WORKS

Handshake Process:

- Establishes secure communication and negotiates encryption keys.
- Authenticates the server (and optionally the client).

Encryption:

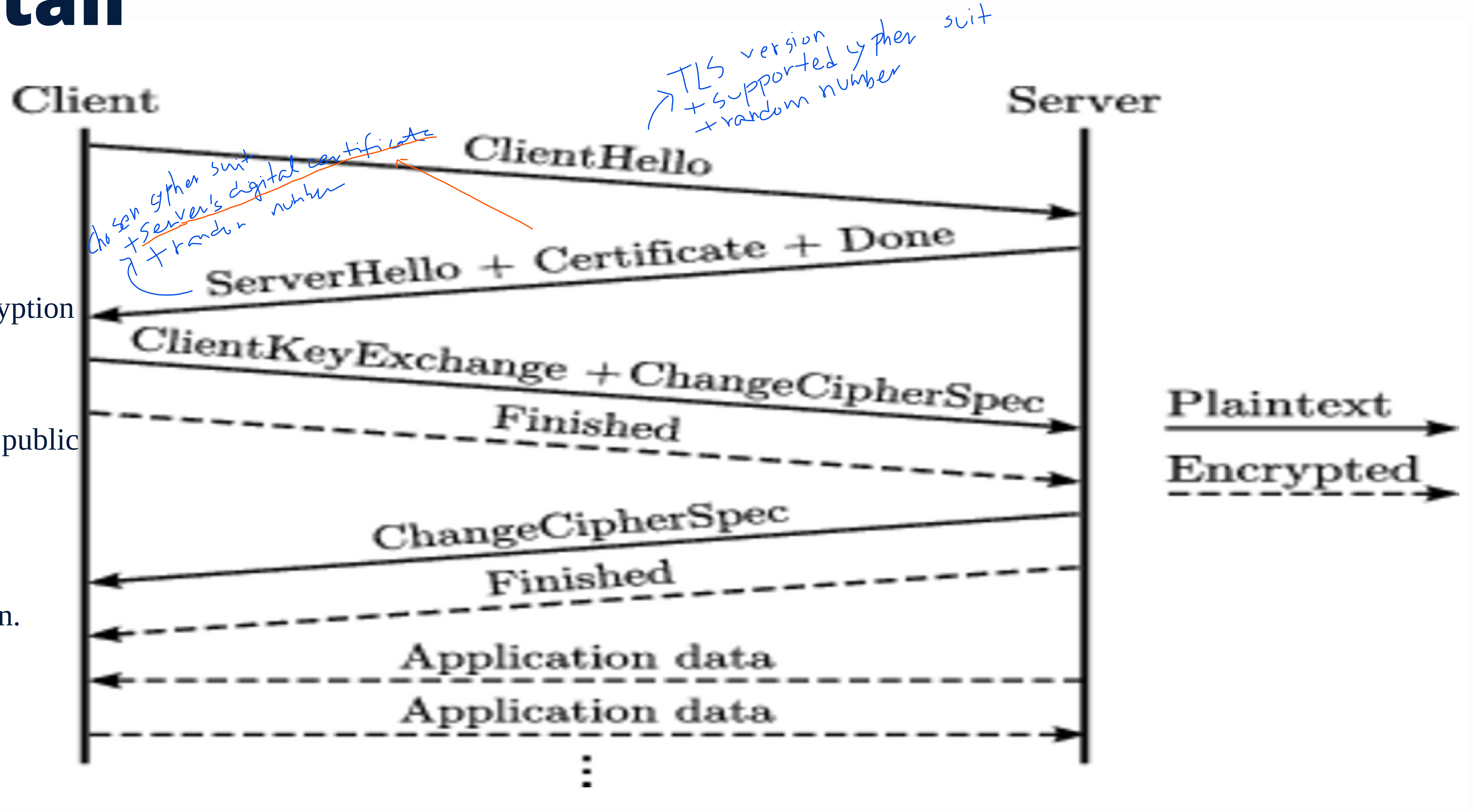
Symmetric encryption secures data transmission.

Integrity Check:

Message Authentication Codes (MACs) verify data has not been altered.

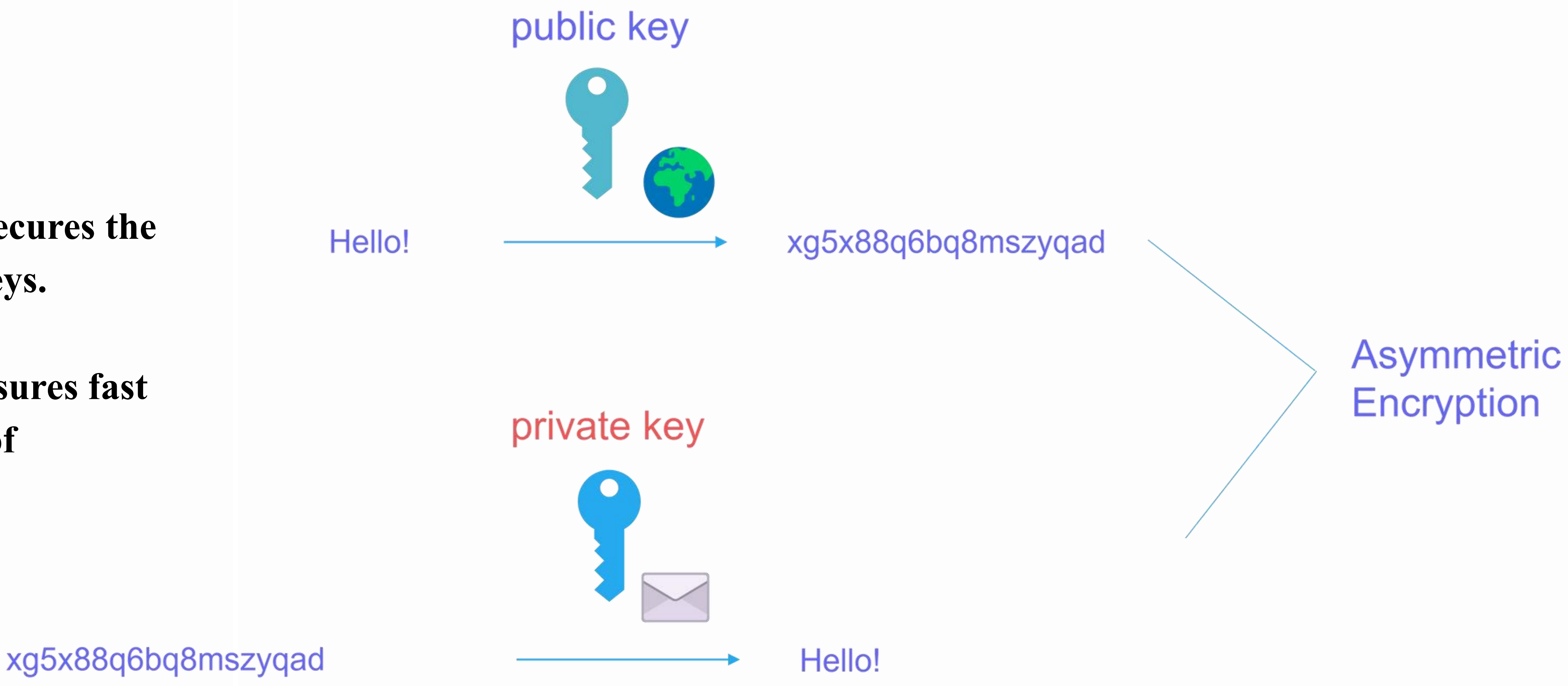
TLS Handshake in Detail

- **ClientHello:**
  - The client sends supported protocols, encryption methods, and random data.
- **ServerHello:**
  - The server responds with selected protocol, encryption method, and random data.
- **Key Exchange:**
  - The server provides its certificate containing the public key.
  - The client validates the certificate.
- **Session Keys:**
  - Symmetric keys are generated for data encryption.
- **Finished:**
  - A secure communication session begins.



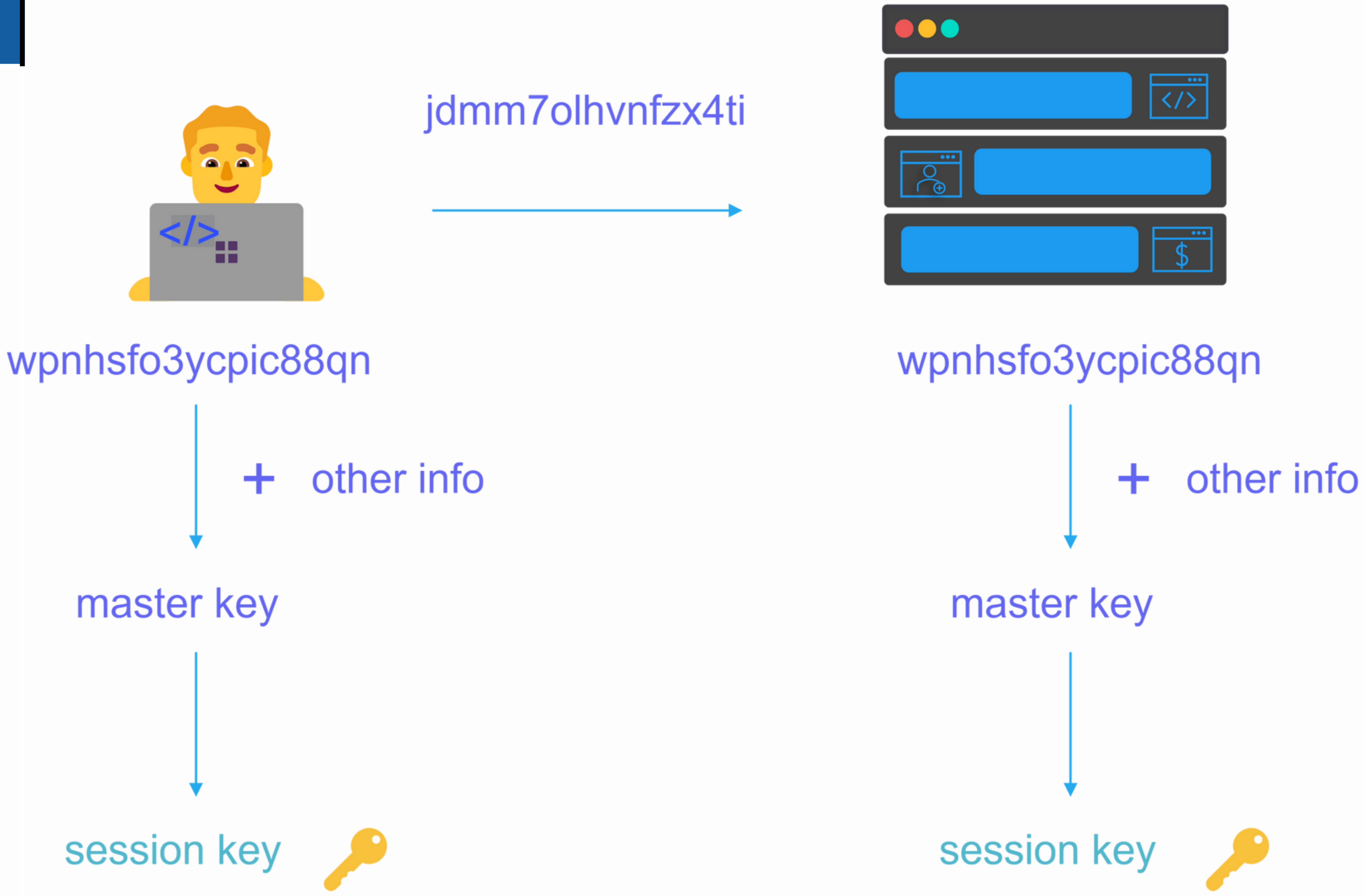
Role of Encryption in TLS

- **During Handshake:**
  - **Asymmetric encryption secures the exchange of symmetric keys.**
- **During Data Transfer:**
  - **Symmetric encryption ensures fast and secure transmission of information.**



Role of Digital Signatures in TLS

- Server Authentication:
  - TLS uses digital signatures to verify the authenticity of server certificates.
- Data Integrity:
  - Ensures transmitted data has not been altered during transit.
- Key Exchange Validation:
  - Confirms the integrity of key exchange messages during the handshake.



Advantages of TLS	Disadvantages of TLS
Data encryption: Ensures confidentiality and integrity of data. **Authentication:** Verifies server and optionally client identity using certificates. **Data integrity:** Prevents tampering during transmission. **Widely adopted**: Compatible with most browsers and platforms.	**Performance impact:** Increases latency and CPU usage. **Cost:** Certificates and their management may be expensive. **Complexity:** Requires configuration and maintenance. **Misconfigured setups:** May lead to vulnerabilities

Applications of TLS

01

Web Browsing:

- TLS secures HTTPS, protecting user data during web sessions.

02

- Email Security:
- Encrypts email transmission protocols like SMTP, IMAP, and POP3.

03

VPNs:

- Ensures private communication over virtual networks.

04

IoT:

- Secures communication in smart devices.

Real-Life Examples of TLS Usage

01

Online Banking

- Description: Banks use TLS to encrypt online transactions, ensuring sensitive data like login credentials, account details, and transaction information remains secure.
- Example: Accessing accounts via online banking platforms like Chase or HSBC.

02

E-commerce Websites

- Description: TLS ensures the protection of customer payment information during online purchases.
- Example: Platforms like Amazon and eBay use HTTPS, powered by TLS, to encrypt payment and personal data.

03

Social Media and Messaging

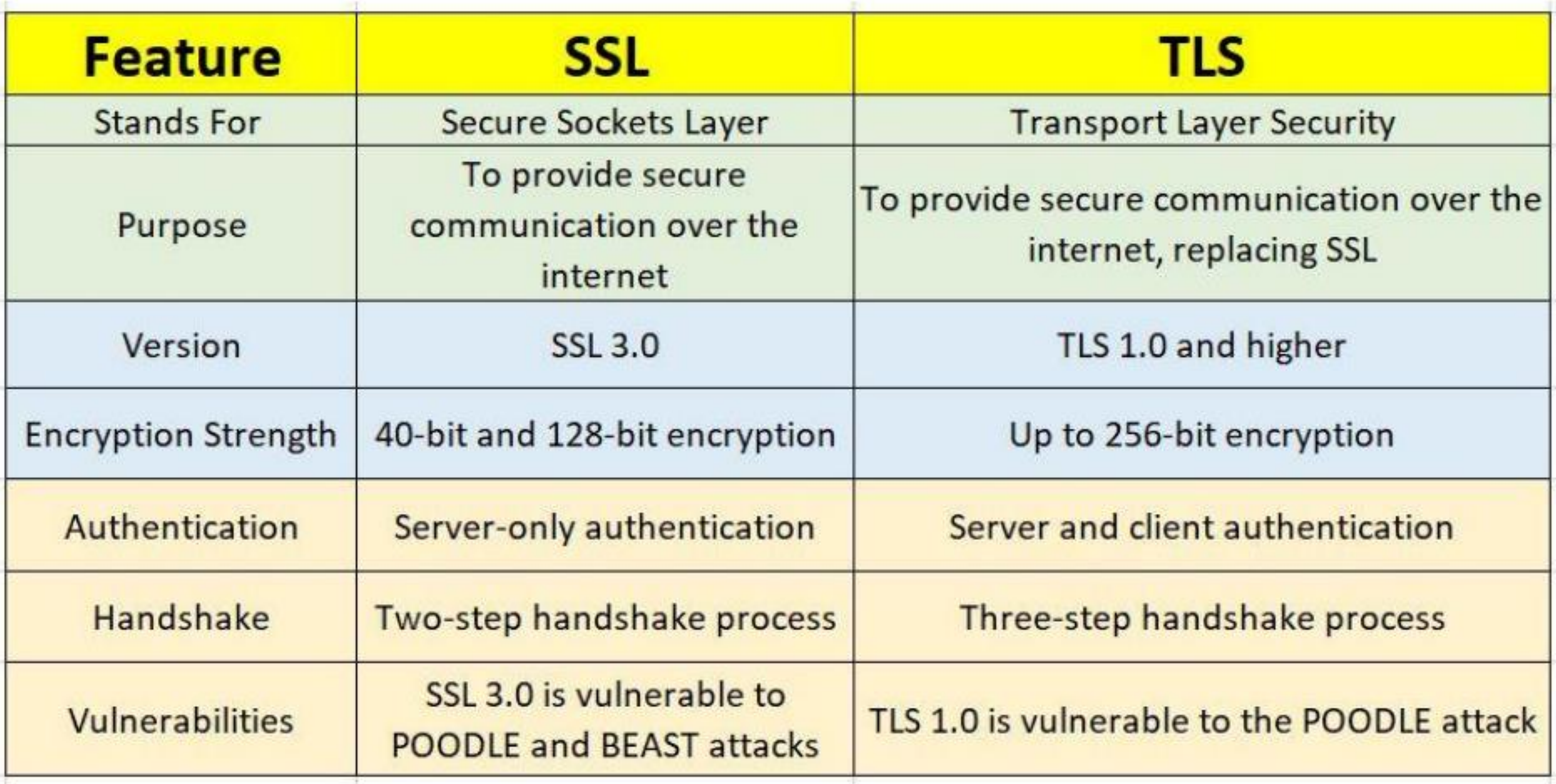
- Description: Social media platforms and messaging apps rely on TLS for secure communication between users.
- Example: Apps like WhatsApp, Facebook Messenger, and Instagram use TLS to protect chats, login details, and media transfers.

04

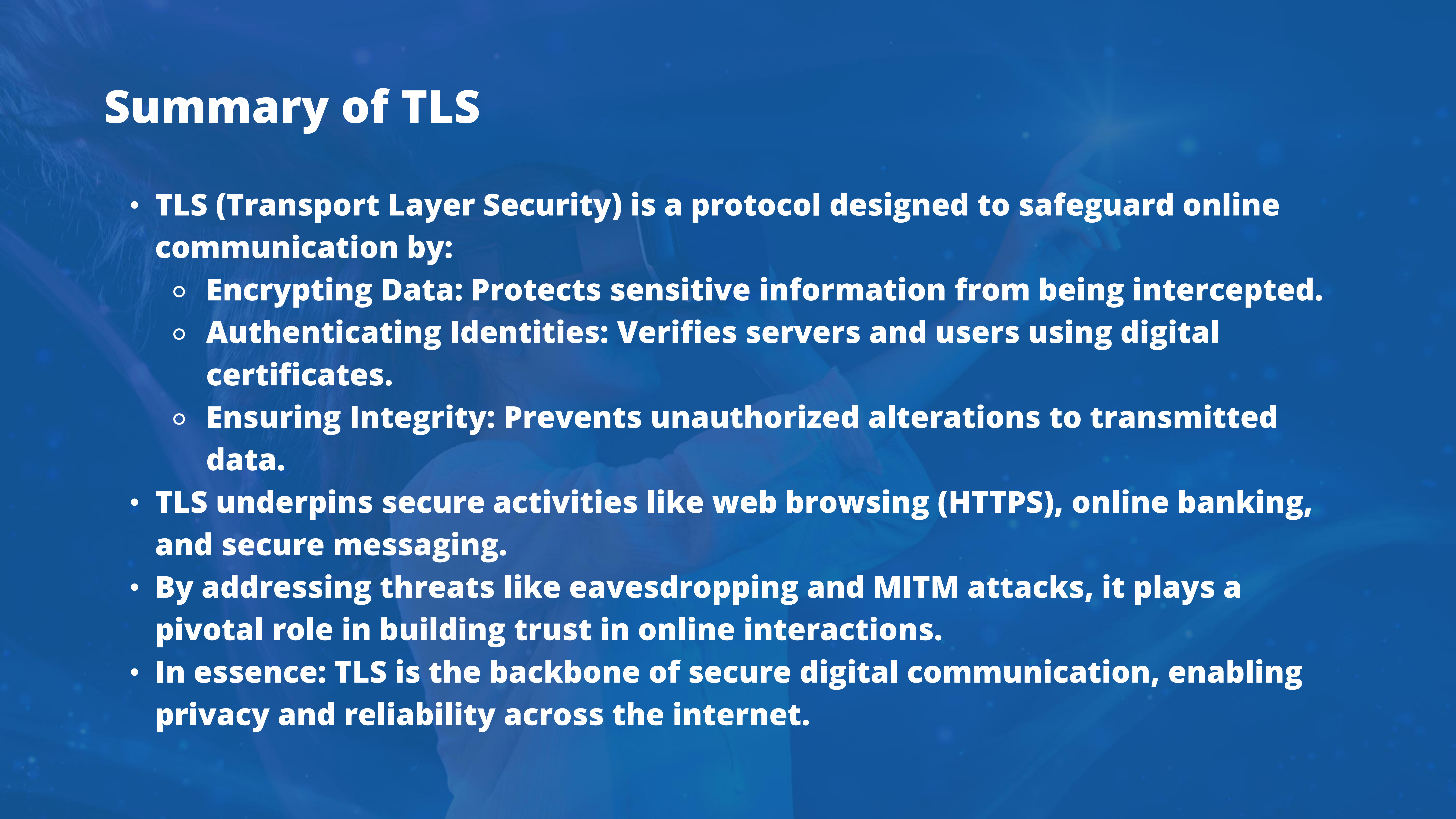
Video Conferencing and Remote Work

- Description: Video conferencing platforms use TLS to secure meetings and prevent eavesdropping or data leaks.
- Example: Services like Zoom, Microsoft Teams, and Google Meet utilize TLS for end-to-end encryption of video and audio data.

Challenges for TLS	Attacks on TLS
• **Certificate management:** Renewals and handling expired certificates. • **Backward compatibility:** Support for older protocols. • **Man-in-the-middle attacks:** Through fake certificates or misconfigurations. • **Revocation issues:** Difficulty in ensuring certificate revocation.	• **BEAST attack:** Exploits vulnerabilities in older TLS versions. • **Heartbleed:** Reads server memory due to a flaw in OpenSSL. • **POODLE attack:** Downgrade attack exploiting SSL 3.0. • **MITM attacks:** Compromising TLS sessions using fake certificates.



Feature	SSL	TLS
Stands For	Secure Sockets Layer	Transport Layer Security
Purpose	To provide secure communication over the internet	To provide secure communication over the internet, replacing SSL
Version	SSL 3.0	TLS 1.0 and higher
Encryption Strength	40-bit and 128-bit encryption	Up to 256-bit encryption
Authentication	Server-only authentication	Server and client authentication
Handshake	Two-step handshake process	Three-step handshake process
Vulnerabilities	SSL 3.0 is vulnerable to POODLE and BEAST attacks	TLS 1.0 is vulnerable to the POODLE attack



Summary of TLS

- TLS (Transport Layer Security) is a protocol designed to safeguard online communication by:
  - Encrypting Data: Protects sensitive information from being intercepted.
  - Authenticating Identities: Verifies servers and users using digital certificates.
  - Ensuring Integrity: Prevents unauthorized alterations to transmitted data.
- TLS underpins secure activities like web browsing (HTTPS), online banking, and secure messaging.
- By addressing threats like eavesdropping and MITM attacks, it plays a pivotal role in building trust in online interactions.
- In essence: TLS is the backbone of secure digital communication, enabling privacy and reliability across the internet.