Introduction to Cryptography

Securing Communication and Data

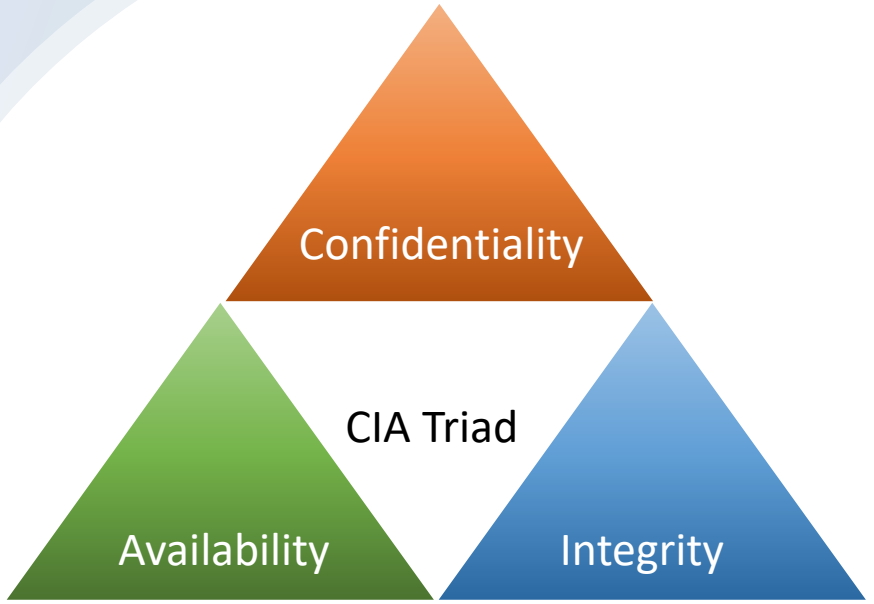
Speaker: Alexandru Chis

Date: 01.02.2024

Introduction to Cryptography

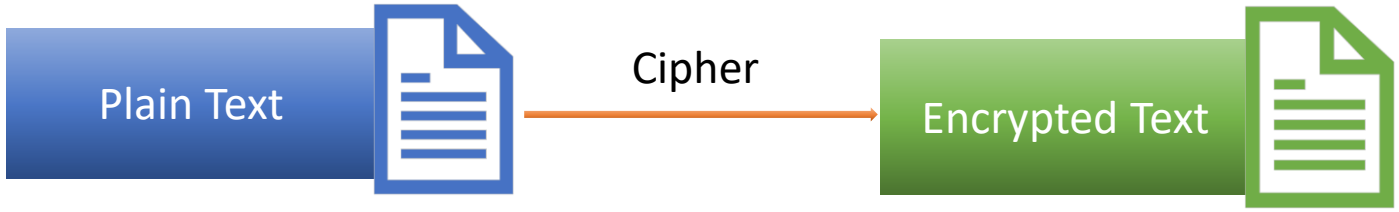
Cryptography = "kryptos" (hidden) + "graphein" (to write).

Cryptography is the science and art of securing communication and data using mathematical techniques and algorithms.

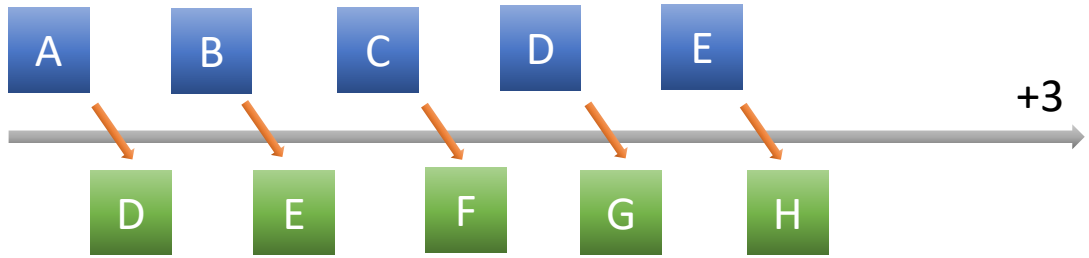


Ciphers and Cryptographic algorithms

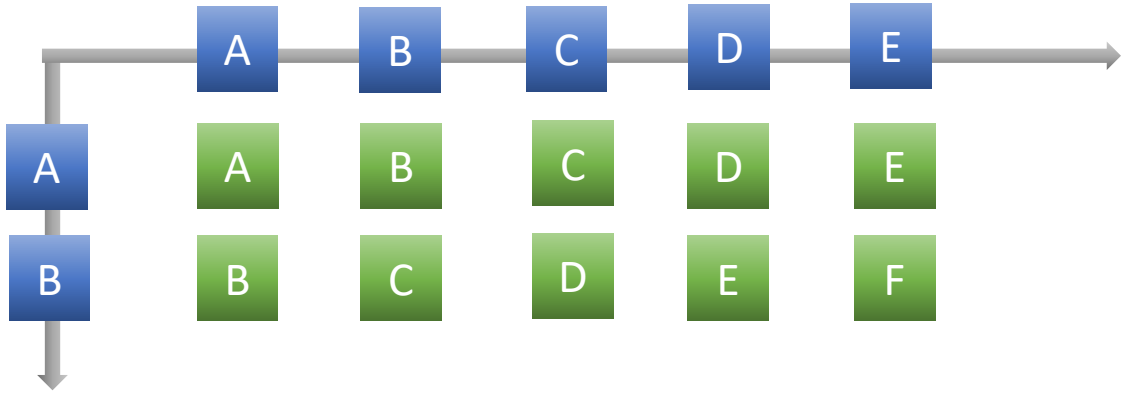
Ciphers are algorithms used to encrypt and decrypt messages, transforming plaintext into ciphertext and vice versa. Here are two fundamental types of cryptographic ciphers:



Monoalphabetic Ciphers:

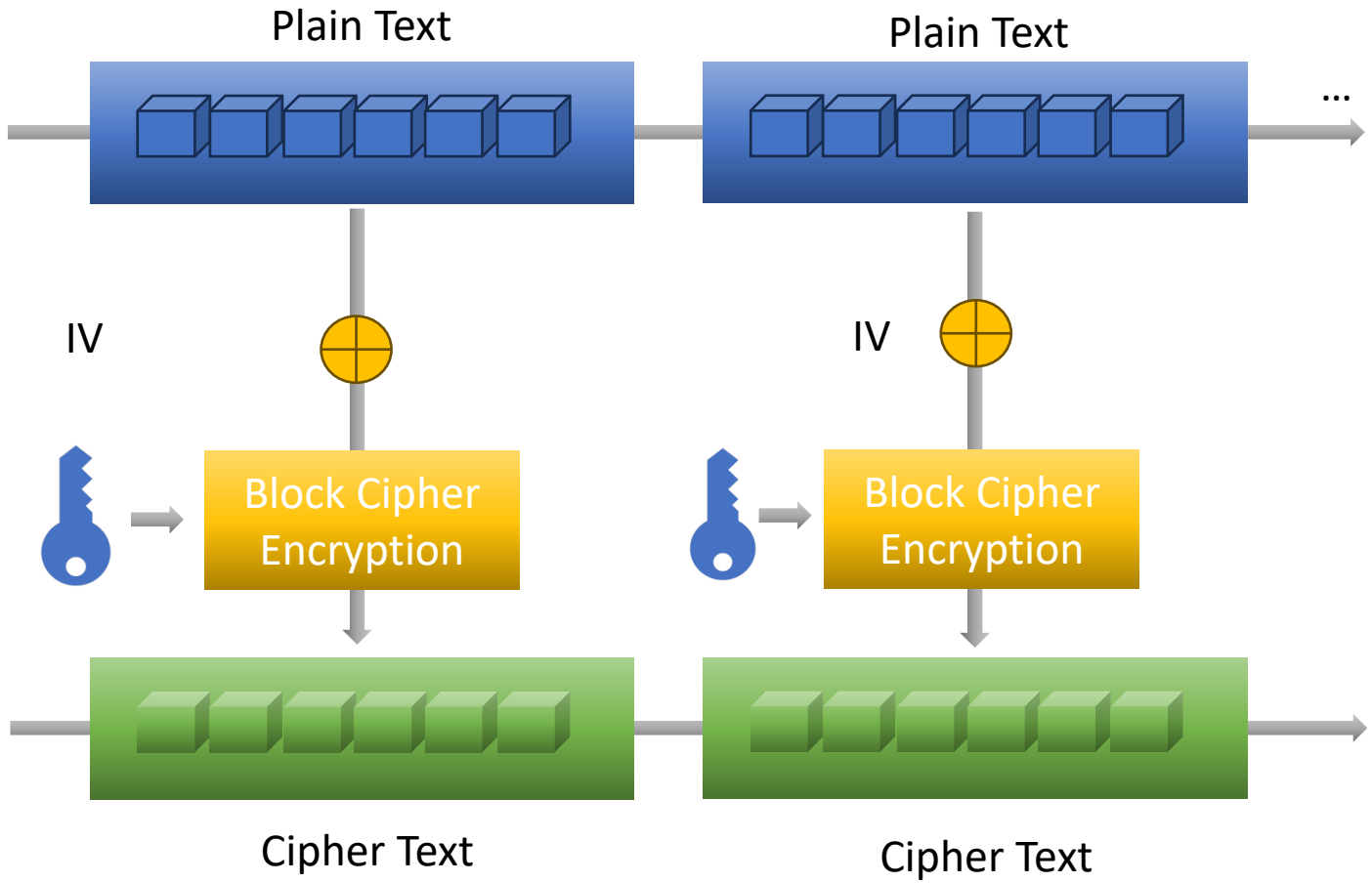


Polyalphabetic Ciphers:



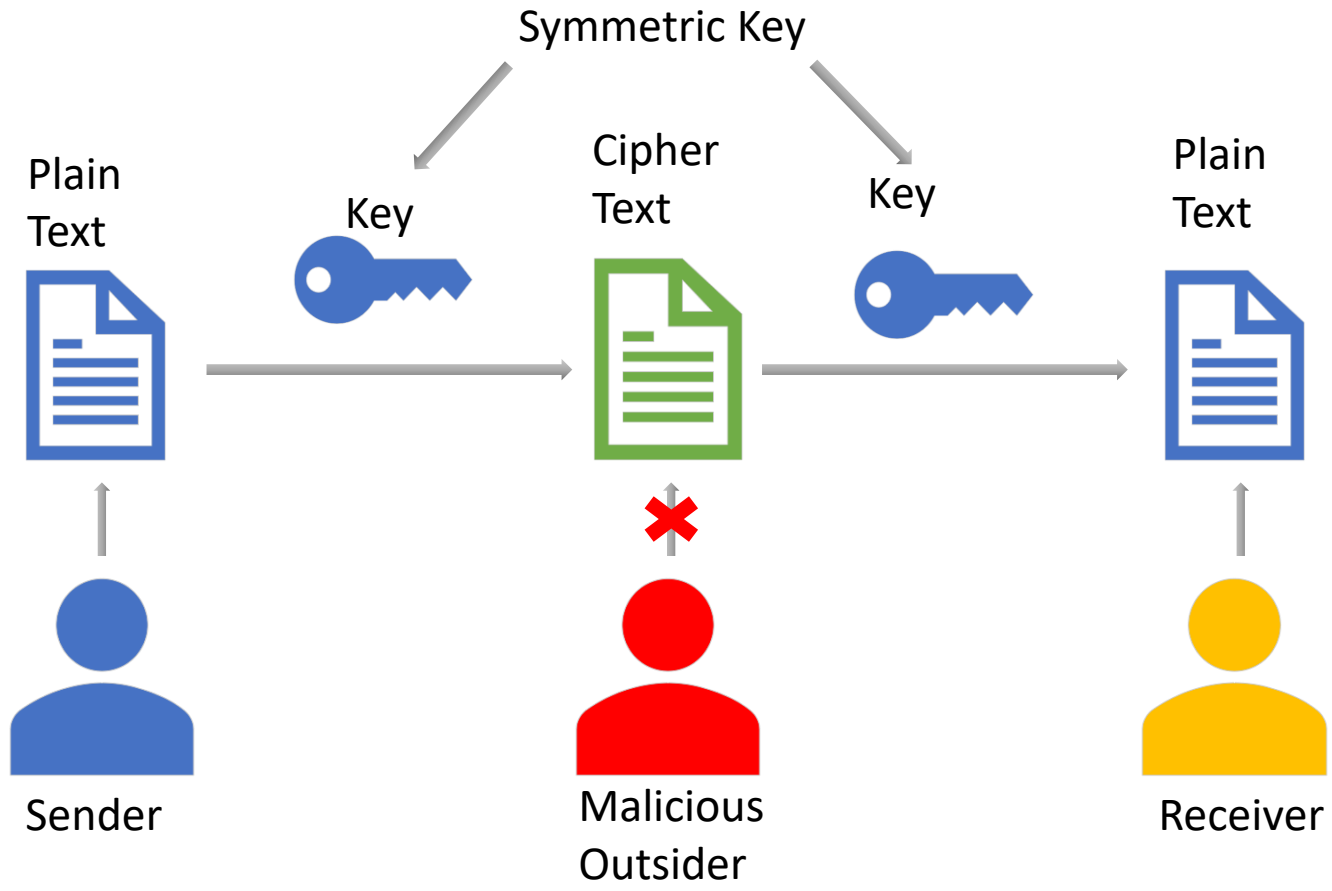
Block Ciphers

Block ciphers are a type of symmetric-key encryption algorithm that processes fixed-length blocks of data at a time, transforming plaintext blocks into ciphertext blocks and vice versa.



Block ciphers can operate in different modes, such as Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Counter (CTR), etc.

Basics of Symmetric Key Encryption



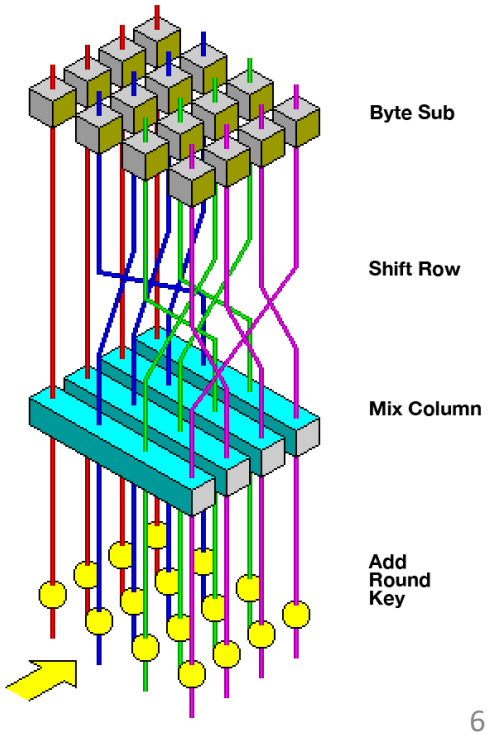
Symmetric Key - Encryption Process

The process of symmetric key encryption involves several key steps to ensure secure communication and data protection:

1. Key Generation
2. Encryption
3. Transmission
4. Decryption

How do you provide the key to the Receiver?

The process of symmetric key encryption involves several key steps to ensure secure communication and data protection:



Limitations of Symmetric Key Encryption

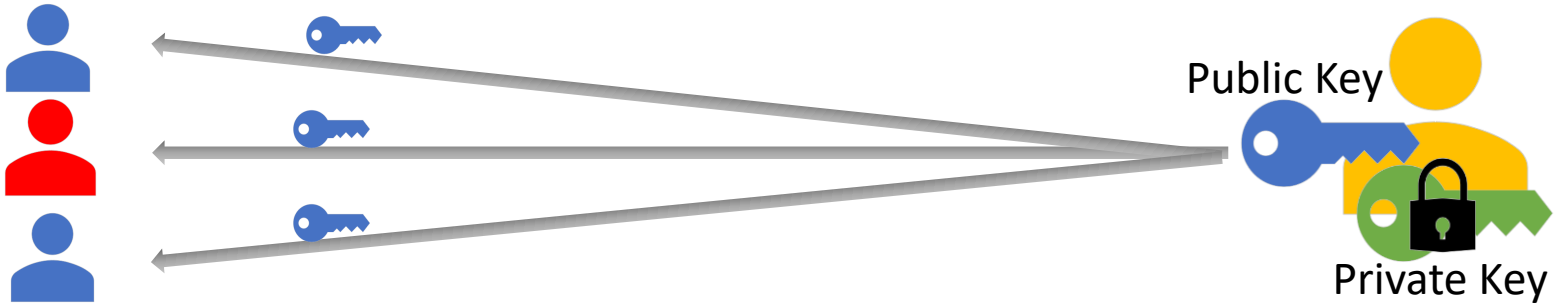
While symmetric key encryption offers speed and efficiency, it also presents several limitations that need to be addressed:

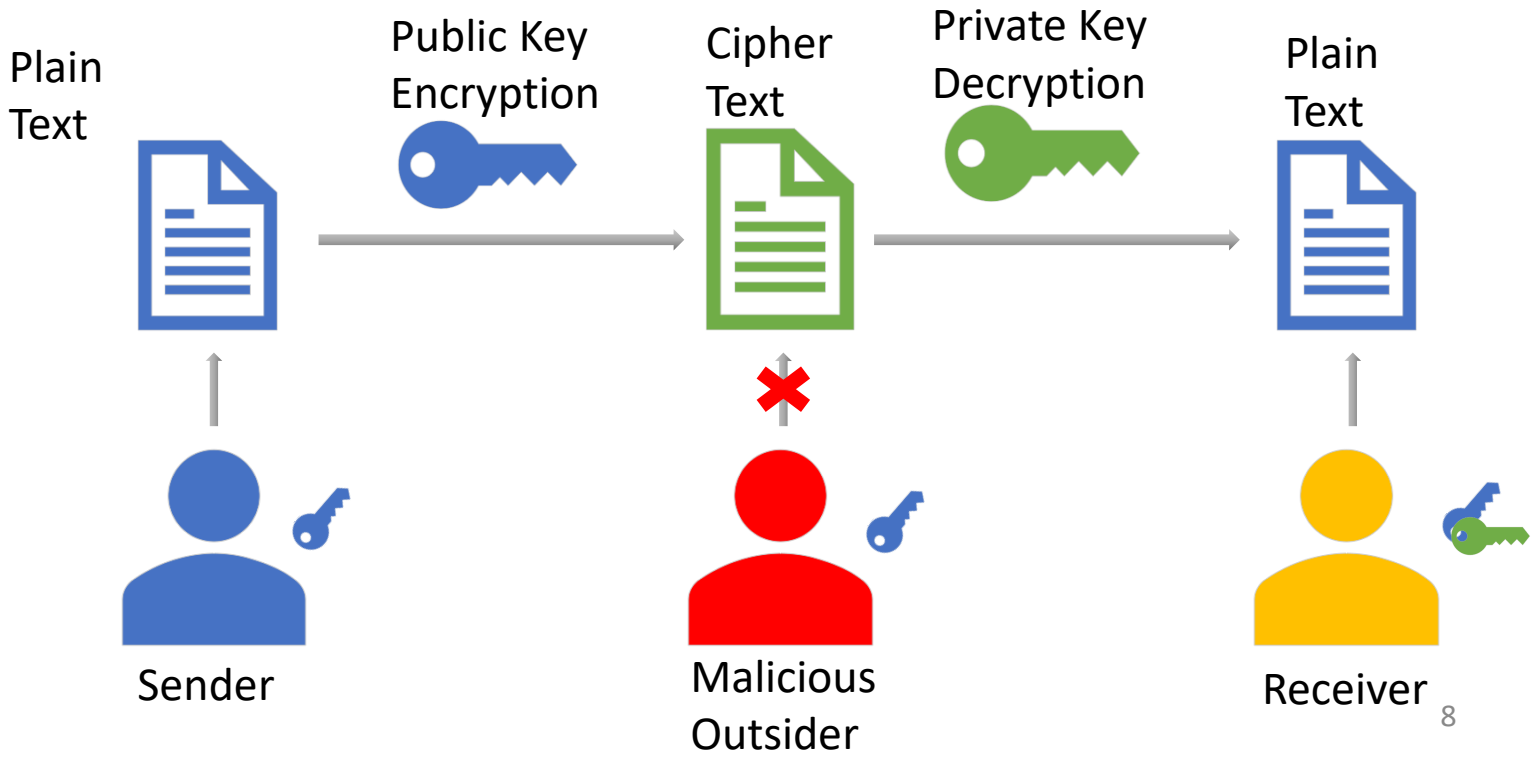
1. **Key Distribution Problem:** How do you transport the key?
2. **Lack of Scalability:** How do you manage all key pairs?
3. **Vulnerability to Key Attacks:** brute-force attacks, cryptographic analysis, or interception

Addressing these limitations led to the development of asymmetric key encryption, which employs a different approach to key management and communication security.

Introduction to Asymmetric Key Encryption

Asymmetric key encryption, also known as public-key encryption, is a cryptographic technique that uses a pair of keys for encryption and decryption: a public key and a private key.





Asymmetric Key Encryption Process

The process of symmetric key encryption involves several key steps to ensure secure communication and data protection:

1. Key Generation
2. Encryption
3. Transmission
4. Decryption

RSA public/private key generation:

1. Select two big prime numbers: *p , q*
2. Calculate *n=p*q*
3. *Φ(n)=(p-1)(q-1)*
4. Select number e such that *GCD(Φ(n),e)=1*, where *1<e<Φ(n)*
5. Compute *d*, where *d*e ≡ 1 % Φ(n)*

Encryption:

$C = M^e \ \% \ n$

Decryption:

$M = C^d \ \% \ n$

Applications of Asymmetric Key Encryption

Asymmetric key encryption offers several key applications in modern cryptography and secure communication:

- Secure Key Exchange
- Digital Signatures
- SSL/TLS Encryption
- Secure Email Communication

Asymmetric key encryption plays a crucial role in enhancing the security and integrity of digital communication channels and transactions. Its versatility and robust security properties make it a cornerstone of modern cryptographic systems.

Advantages and Disadvantages of Asymmetric Key Encryption

Asymmetric key encryption offers several advantages over symmetric key encryption, but it also has its own set of limitations:

Advantages:

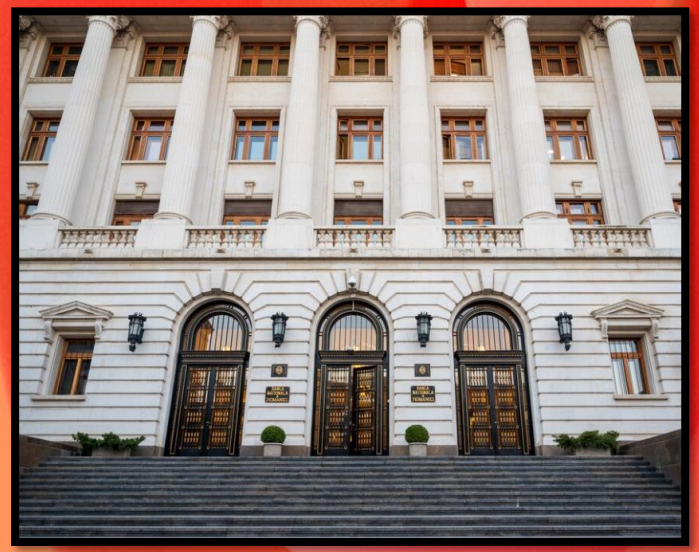
- Key Distribution
- Scalability
- Digital Signatures

Disadvantages:

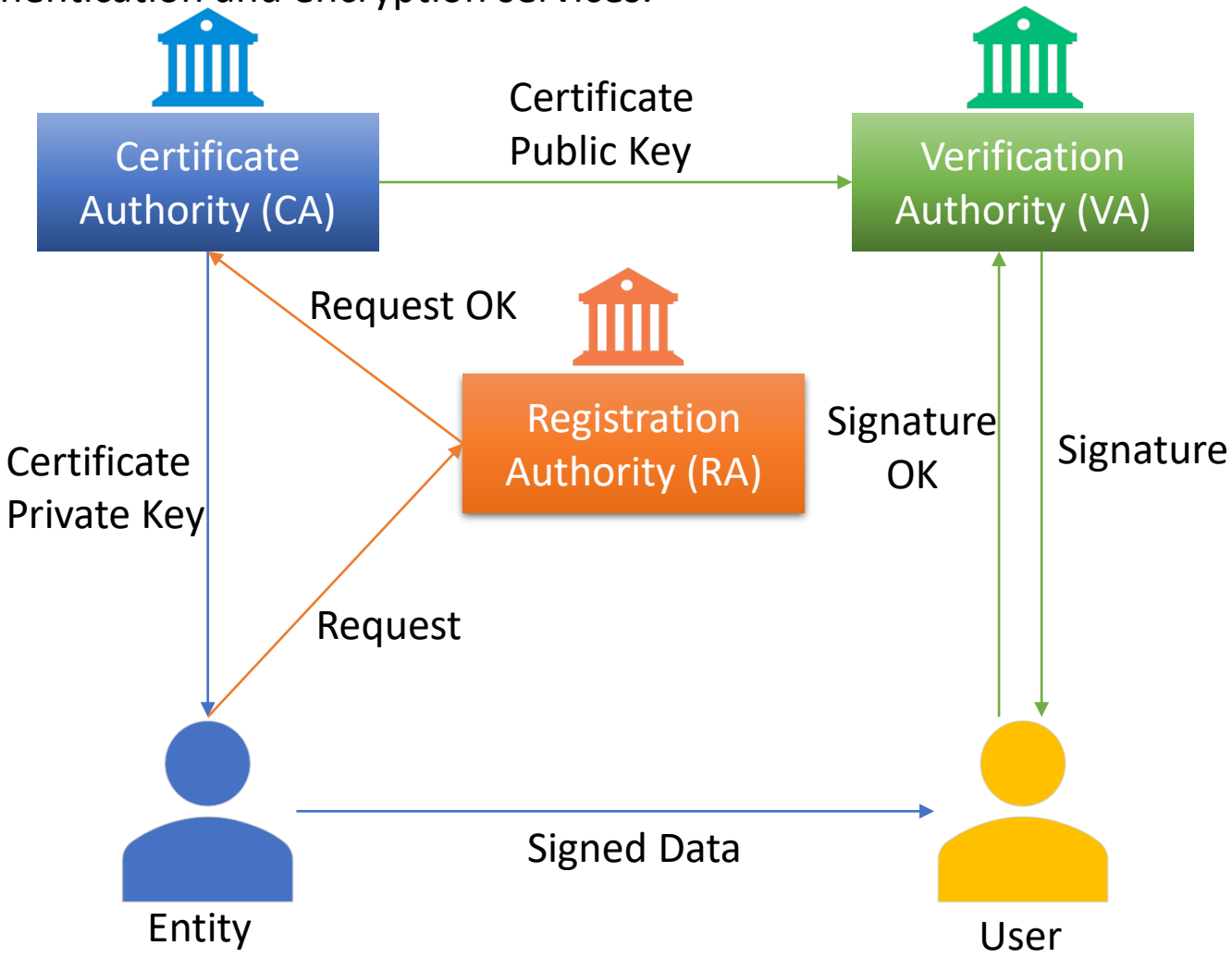
- Performance Overhead
- Key Length
- Key Management

Despite these limitations, asymmetric key encryption remains a cornerstone of modern cryptographic systems, offering a versatile and secure approach to secure communication and data protection.

Public Key Infrastructure (PKI) Overview



Public Key Infrastructure (PKI) is a comprehensive framework that facilitates secure communication and data exchange in a networked environment. It serves as the foundation for managing digital certificates and enabling secure authentication and encryption services.



Role of Certificate Authorities (CAs)

Certificate Authorities (CAs) play a pivotal role in the Public Key Infrastructure (PKI) framework, ensuring the integrity and security of digital certificates and enabling trusted communication and authentication services.

Functions of Certificate Authorities:

1. Issuance of Digital Certificates
2. Certificate Revocation (CRLs)
3. Key Escrow and Recovery
4. Certificate Policy Enforcement

Certificate Authorities are trusted entities that form the cornerstone of secure communication and authentication services in modern digital environments. Their role in verifying identities, issuing digital certificates, and upholding security standards ensures the integrity and confidentiality of digital transactions and communications.

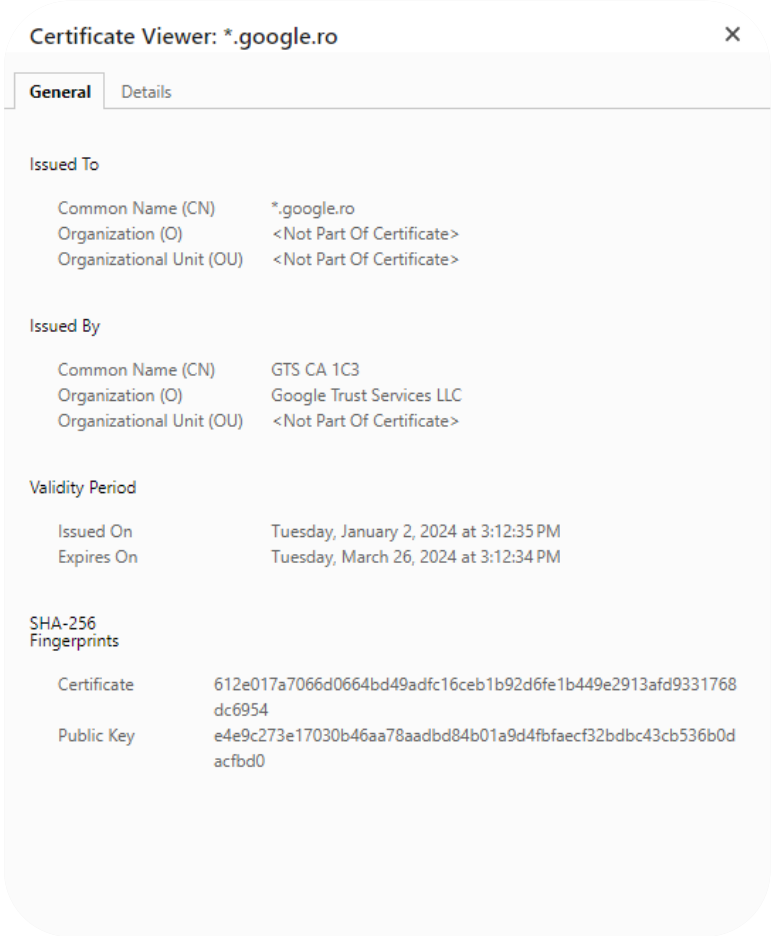
Digital Certificates

Enable Secure Communication

Establish Trust

Identity Verification

Digital certificates are cryptographic credentials issued by Certificate Authorities (CAs) that bind an entity's identity to its public key.



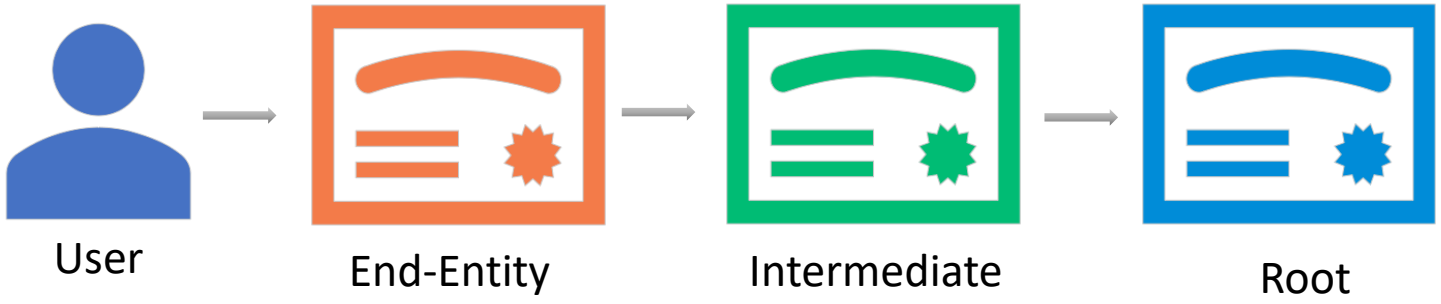
Contents of a Digital Certificate:

1. Subject Information
2. Public Key
3. Issuer Information
4. Certificate Validity Period
5. Digital Signature

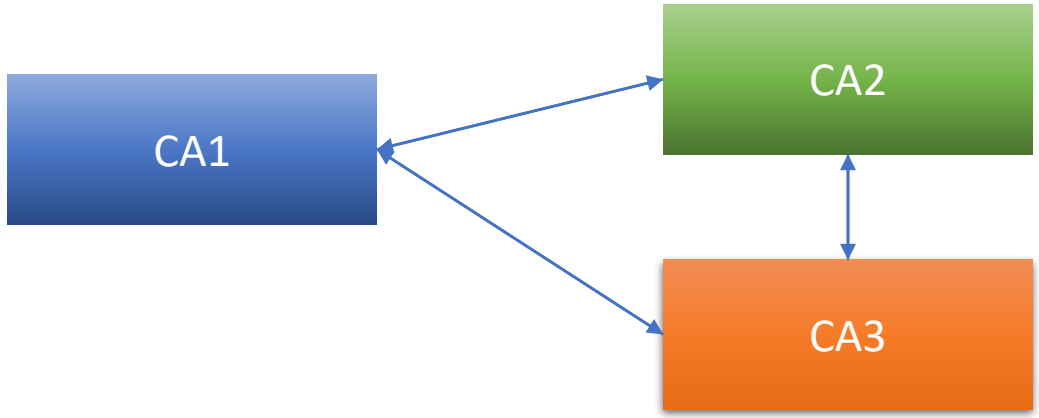
Certificate Chains and Trust Hierarchies

Certificate chains and trust hierarchies are integral components of the Public Key Infrastructure (PKI) framework, enabling the establishment of trust relationships and the verification of digital certificates.

Building Trust Chains



Trust Hierarchies



Applications of Digital Certificates

Digital certificates are versatile cryptographic credentials that find applications across various domains and industries. They play a crucial role in securing digital transactions, authenticating users and devices, and ensuring data integrity.

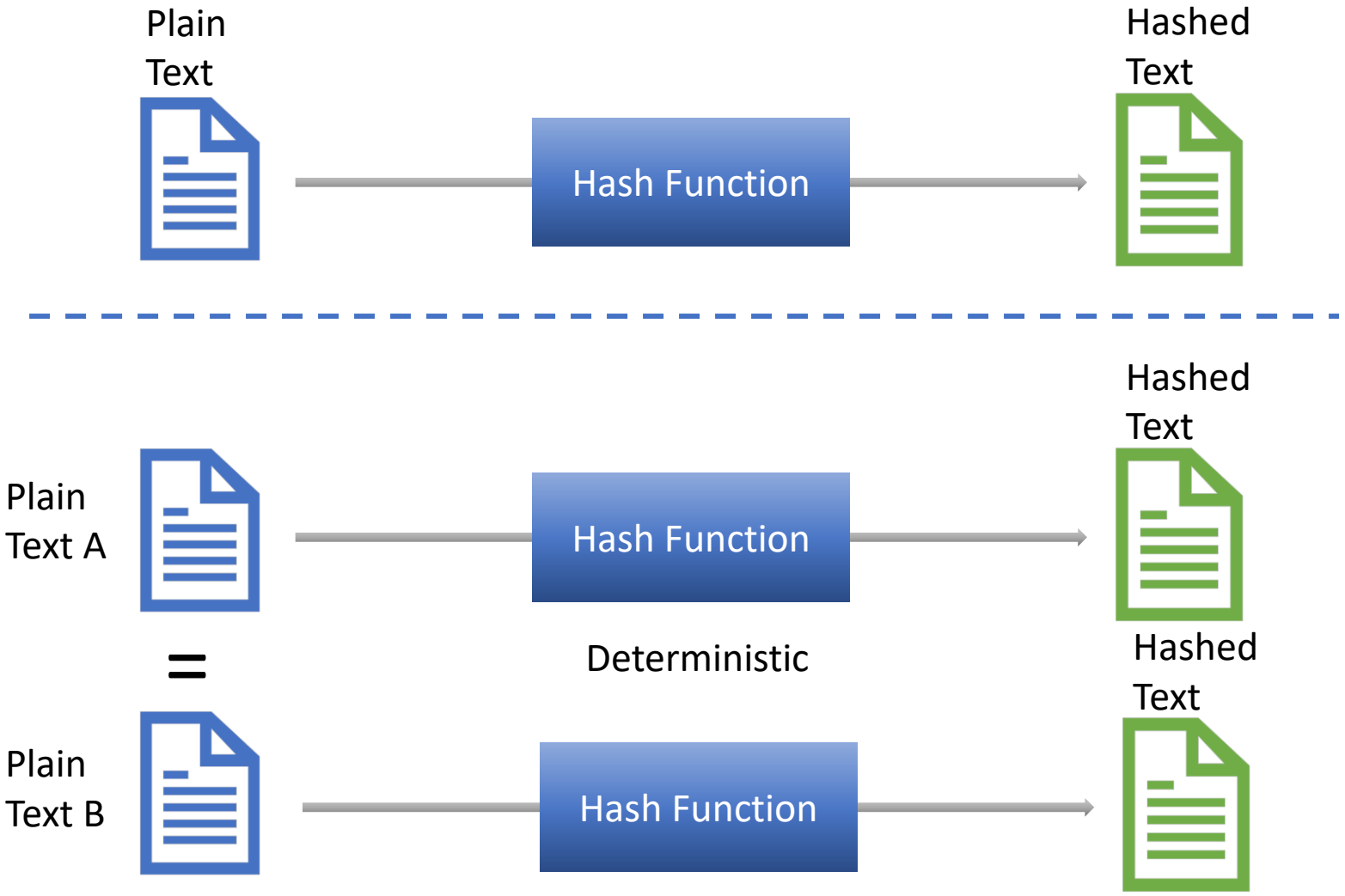
Key applications of digital certificates:

1. Secure Web Communication (HTTPS
2. Email Encryption (S/MIME)
3. Code Signing
4. Document Signing
5. Client Authentication

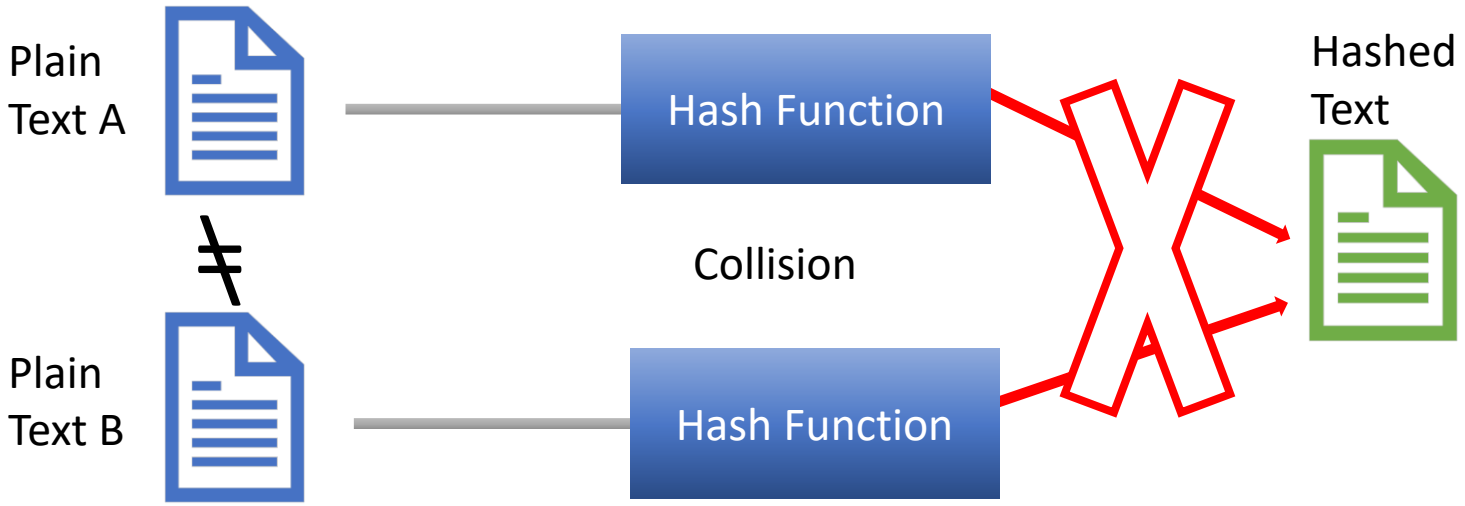
Digital certificates serve as trust anchors in the digital realm, enabling secure communication, data exchange, and transactional integrity. Their widespread adoption across industries underscores their importance in modern cybersecurity practices and standards.

Cryptographic Hash Functions

Cryptographic hash functions are essential cryptographic tools used to ensure data integrity, verify message authenticity, and securely store passwords. These functions generate fixed-size hash values (digests) from variable-length input data, with the following key properties:



Applications of Cryptographic Hash Functions



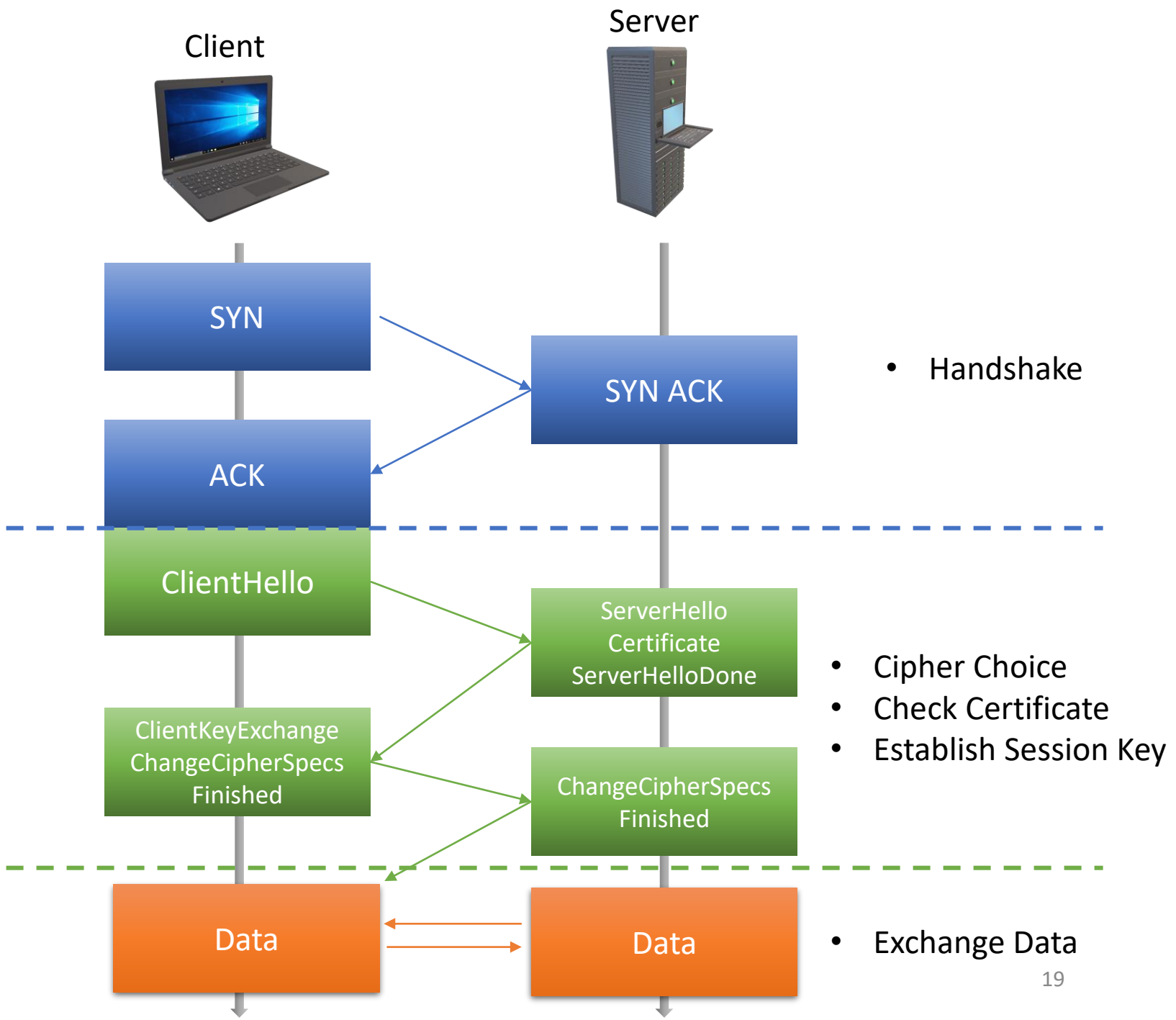
Cryptographic hash functions play a vital role in various applications where data integrity, authentication, and security are paramount.

Key applications of cryptographic hash functions:

- Data Integrity Verification
- Password Storage
- Digital Signatures
- Blockchain Technology
- Message Authentication Codes (MACs)

18

SSL/TLS (Secure Sockets Layer/Transport Layer Security)



Conclusion

In conclusion, cryptography serves as the cornerstone of modern cybersecurity, providing essential tools and techniques to secure digital communication, data transactions, and networked systems.

Throughout this presentation, we have explored the fundamental concepts of cryptography, including:

- Symmetric and asymmetric key encryption techniques
- Public Key Infrastructure (PKI) and digital certificates
- Cryptographic hash functions and their applications
- Cryptographic protocols for securing communication channels

Cryptography enables organizations and individuals to establish trust, ensure confidentiality, and protect against unauthorized access and data tampering. By implementing robust cryptographic measures, we can safeguard sensitive information, mitigate cybersecurity risks, and uphold the integrity of digital transactions and communications.

As technology continues to evolve, cryptography remains a critical component in addressing emerging cybersecurity challenges and safeguarding digital assets in an interconnected world. By staying informed and adopting best practices in cryptography, we can build resilient and secure systems that withstand evolving threats and vulnerabilities.

Thank you!

Contact: **Alexandru Chis**
E-mail: **alexandru.chis@unitbv.ro**