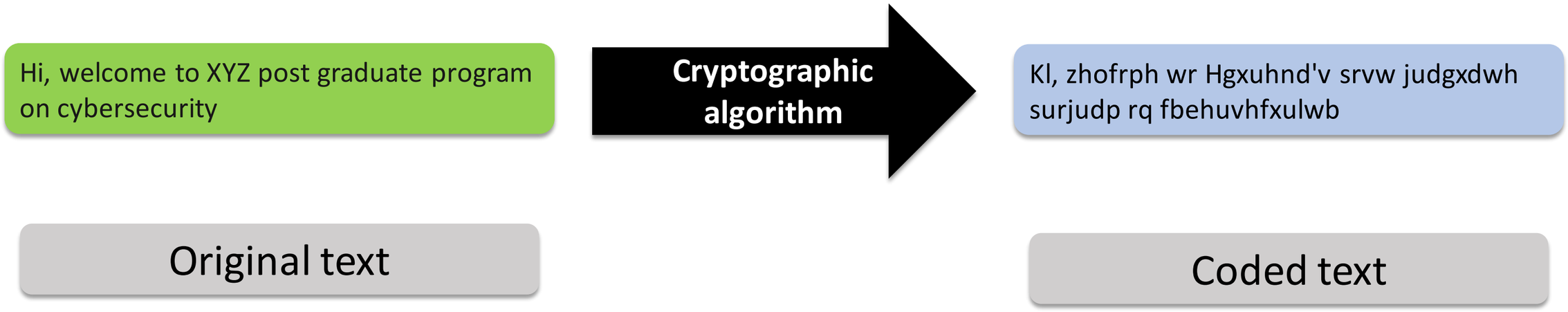
Introduction to Cryptography and Encryption Methods

Ajit Pal Singh Wadhawan ajit-teaches.com
BE, MBA, CISA,CISM,CISSP,CCSP,CRISC, CEH, Security+, ISO 27001 LA
Email- Apsw2015@gmail.com
Mo – 9650339997
https://ajit-teaches.com/

What is Cryptography?

Cryptography is the study of securing communication and data with algorithms to prevent exposure to an unintended party

It is the science of altering valuable information for secrecy



Features of Cryptography

Data Confidentiality

Confidentiality and privacy of data is maintained through ***encryption***. The encrypted data is practically useless to an adversary without the decryption key

Authentication

Authenticity of the message is verified through ***digital signatures,*** which confirms the identity of the sender

Data Integrity

To preserve the ***integrity*** of the message, cryptography uses ***hashing algorithms*** (the same message must always result in the same hash)

Non-Repudiation

Cryptography ensures ***non-repudiation*** through ***digital signatures or digital certificates*** where a user cannot deny sending the message

Cryptographic Terminologies

Plaintext: Original message which is intended to be hidden from adversaries

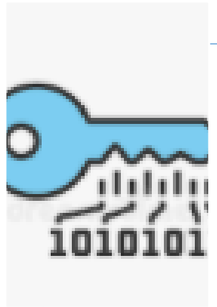
Key: A value that is used to encrypt/decrypt any given message

Encryption algorithm: A mathematical algorithm which converts plaintext to ciphertext using the key

Ciphertext: Cryptic version of the plaintext that was created by an encryption algorithm

Decryption algorithm: An algorithm that decrypts the ciphertext using the key

Cryptography Key



Key

- Also cryptovariable. Sequence that controls the operation of the cryptographic algorithm. Secret or Public

Key Clustering

- Instance when two different keys generate the same ciphertext from the same plaintext using the same algorithm

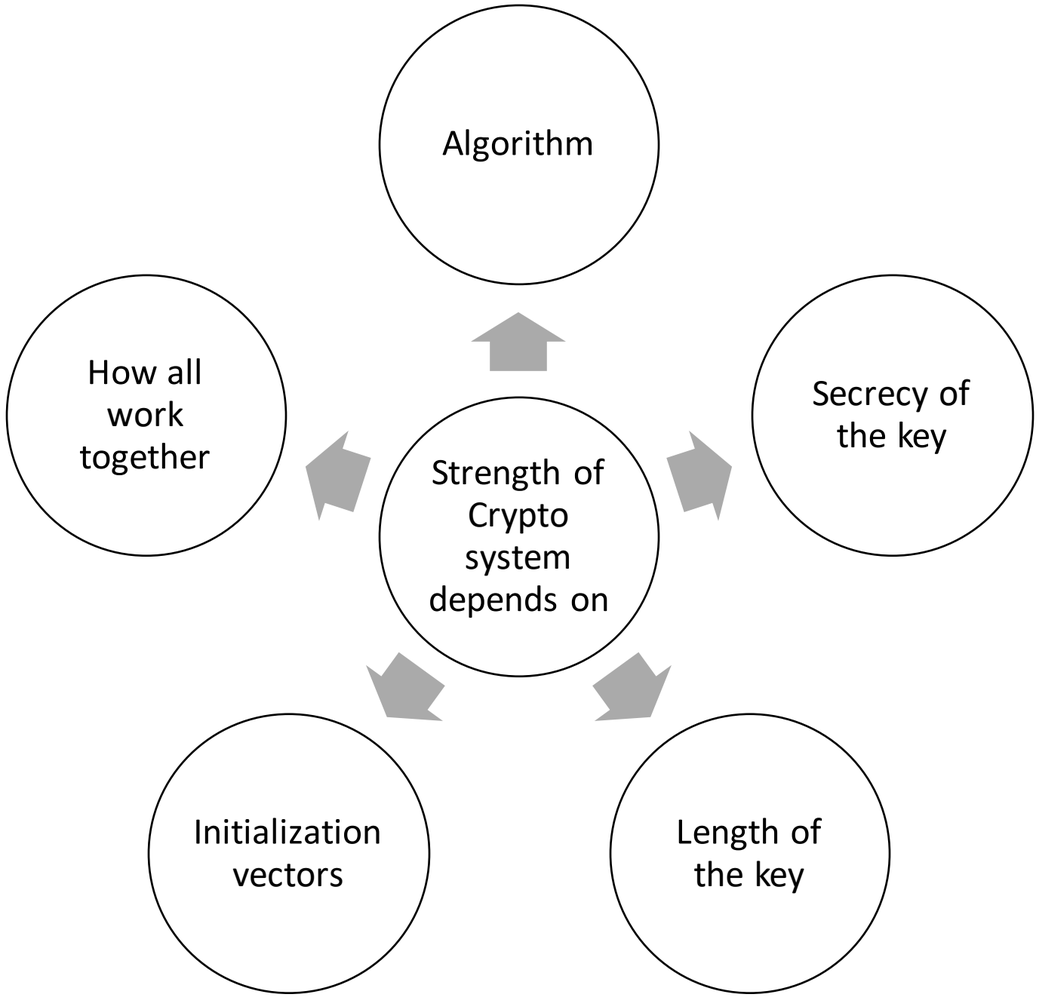
Keyspace

- Total number of possible values for keys in a cryptographic algorithm or password. i.e., key spacefor a 8-bit key would be 256.

Kerchoffs' principle

- Concept that an algorithm should be known and only the keys should be kept secret

Strength of Cryptosystem



Work factor

- An estimate of the effort and resources it would take an attacker to penetrate a cryptosystem

Brute force attack is used to break a cryptosystem.

A good cryptosystem should be cost efficient and less time-consuming.

Cryptosystem Elements

Cryptosystem Elements

- Use an algorithm without flaws
- Use a large key size
- Use all possible values within the key space as randomly as possible
- Protect the actual key

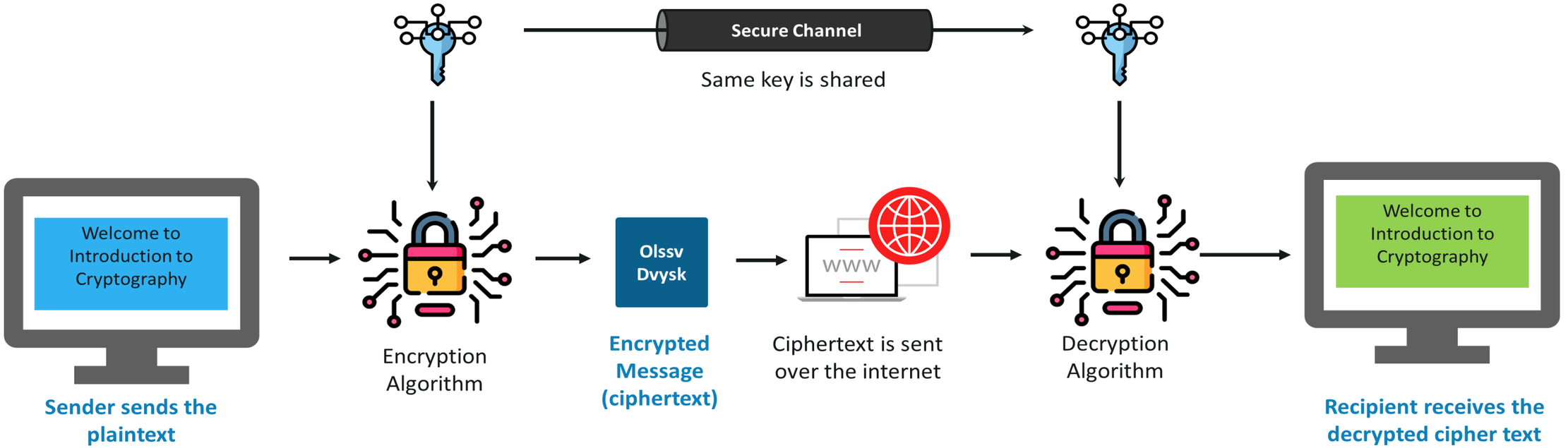
Encryption Methods

Symmetric Key Algorithm

Asymmetric Key Algorithm

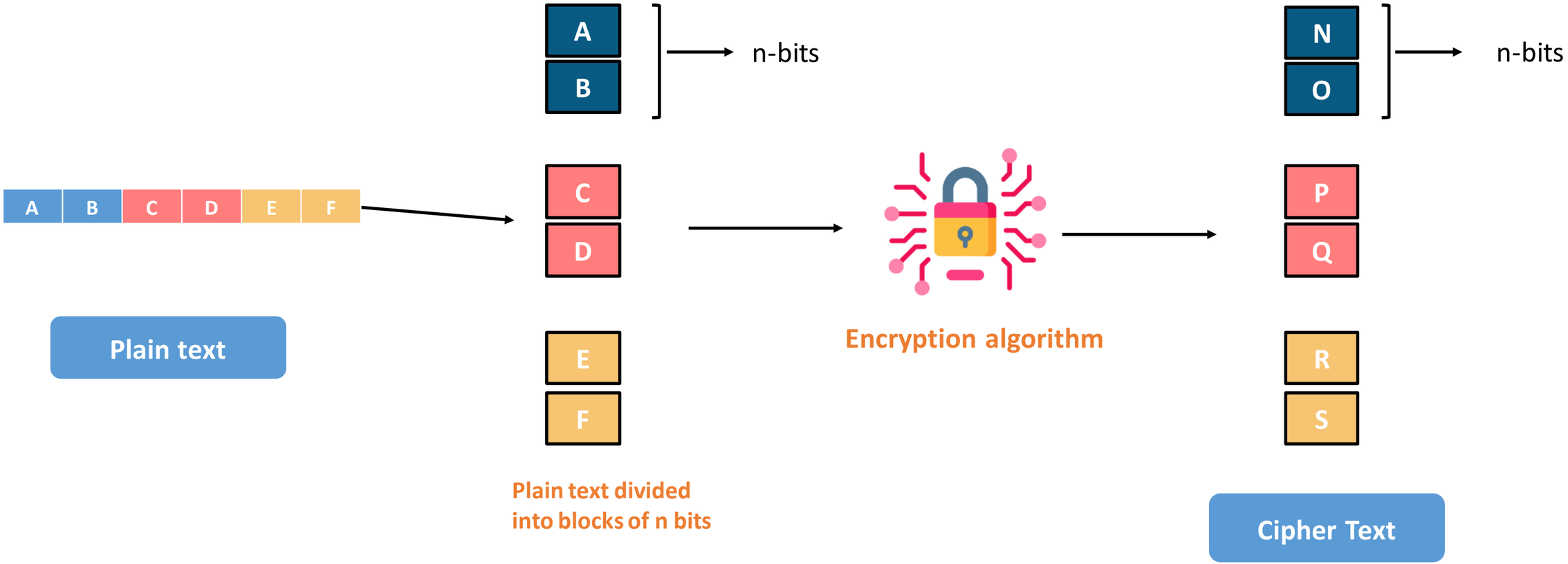
Symmetric Cryptography

- **Same key is used for encryption and decryption**
- The sender and receiver must possess the shared key
- **Symmetric encryption can be executed using block cipher or stream cipher**
- Examples – 3DES, AES (Advanced Encryption Standard)
- Number of keys = N(N-1)/2, whereas N= Number of People



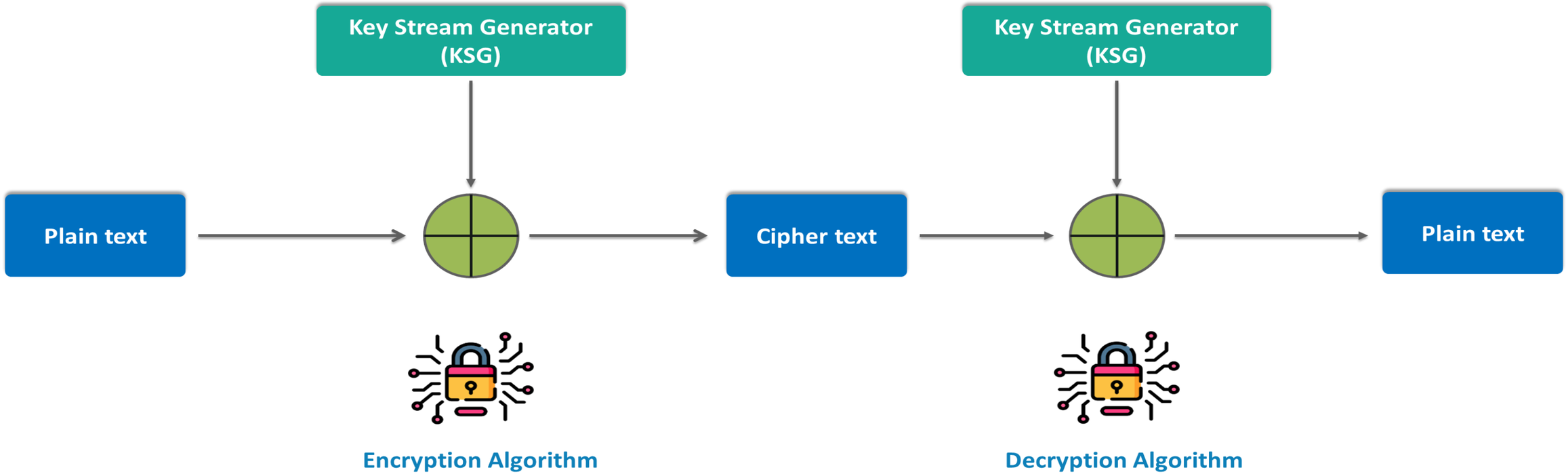
Block Ciphers

In a block cipher, a block of plaintext is divided into n bit blocks, and then the cryptographic algorithm is applied to these blocks at once as a group to generate ciphertexts of equal length. A block normally consists of a contiguous set of bits that is a power of 2 in size



Stream Ciphers

A stream cipher encrypts data one bit, one byte, or one character at a time. A keystream generator outputs a stream of bits. This keystream is XORed with a stream of plaintext bits to produce the stream of ciphertext bits. At the decryption end, the ciphertext bits are XORed with an identical keystream to recover the plaintext bits



Block vs Stream Ciphers

Block Cipher	Stream Cipher
Conversion is done one block at a time	Conversion is down one byte, one bit or one character at a time
Implements both, confusion and diffusion	Strictly based on confusion
Same key is used to encrypt each block	Different key is used to encrypt each bit
Reverse engineering the cipher text is extremely difficult	Reverse engineering comparatively simple as it uses XOR for encryption
Popular implementation include DES, AES	Popular implementations include RC4
A small change in the plain text, completely changes the cipher text	Changes may be predictable

Symmetric Cryptography Is Used In

ATM's to authorize cardholders and perform other banking transactions

File encryption to encrypt files and convert them into ciphertext

WiFi Security to authenticate devices to Wi-Fi access points

Mobile security to help IT companies & users protect data on mobile devices

Database encryption to encrypt data within a database into ciphertext

Symmetric Keys Algorithms

Algorithm	Block Size	Key length	Comments
DES	64bit	56bit + 8 bit parity	16 rounds of processing
2DES	64bit	112bit	Compromised by Meet-in-the-Middle attack
3DES	64bit	168bit	
Rijndael	128,192,256bits	128,192,256bits	Performs variable rounds of operation
IDEA	64bit	128bit	8 rounds transposition and substitution Used in PGP
CAST	64bit	40 to 128bits	
SAFER	64 to 128bit	64 to 128bit	A version used in Bluetooth
Blowfish	64bit	Variable key size	
Twofish	128bit	128, 192, 256 bits	
RC5	16,32,64bits	0 to 2040 bits	
AES	128bit	128, 192, 256 bits	

Session Keys

Session Key

- Single use symmetric key that is used to encrypt/decrypt communication between two users for a single session
- Its much secure than static symmetric keys
- Peers decide on the session key and continue to use it till the session is over
- Eavesdropping is difficult, breaking the keys is futile

Introduction to Asymmetric Cryptography

Asymmetric Cryptography.

- Both sender and receiver have a public key and a private key
- In asymmetric cryptography, two keys are used that are linked mathematically, but are mutually exclusive. One for encryption and other for decryption.
- Asymmetric encryption is also called public key encryption as one key is made public.
- Pair of keys are required for encryption/decryption
- These keys are mathematically related and Each key is used to encrypt/decrypt
- Public key is usually shared while private key is secured by the owner
- Examples: RSA, Diffie-Hellman, Elliptic curve cryptosystem (ECC), El Gamal, Digital signature algorithm (DSA).

Communication takes place in two formats

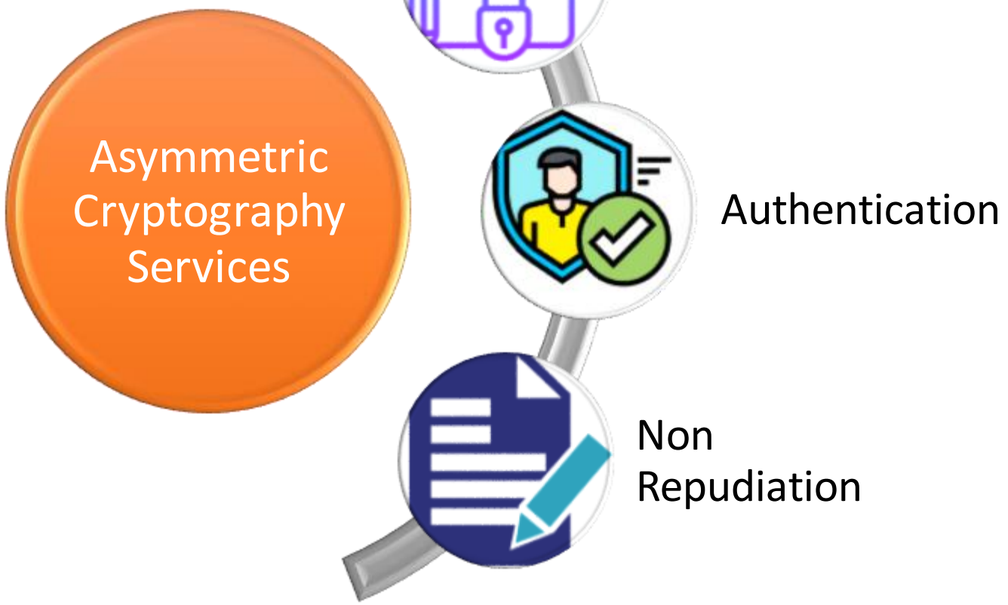
Secure Message format

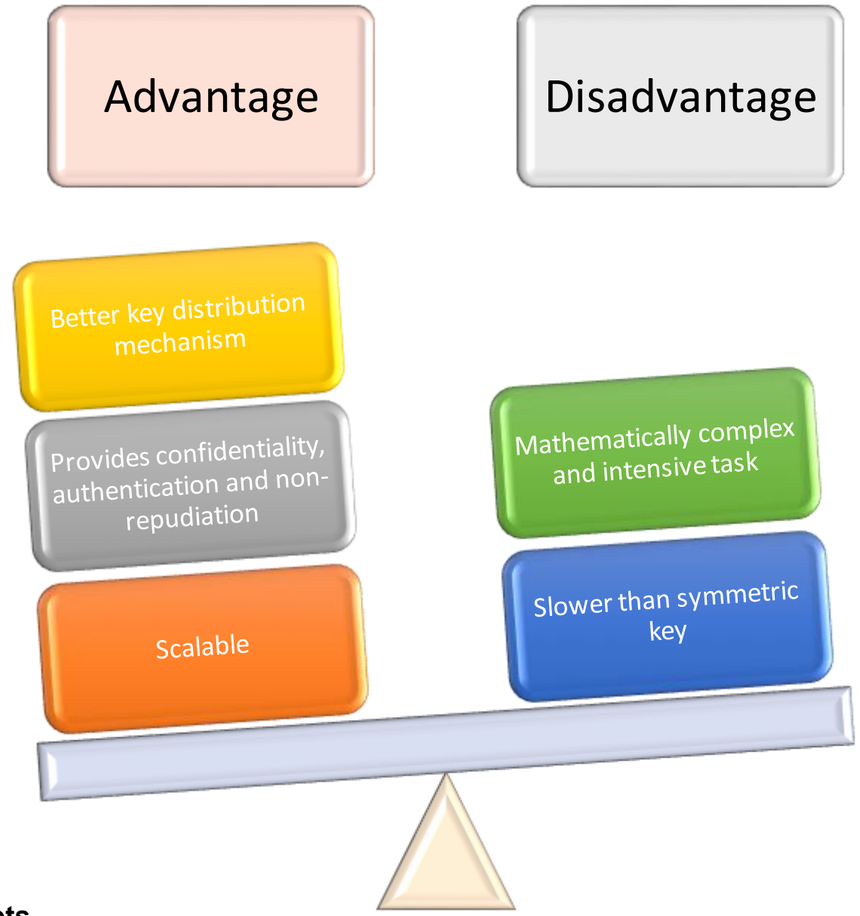
- Confidentiality
- Message is encrypted with receiver's public key

Open Message format

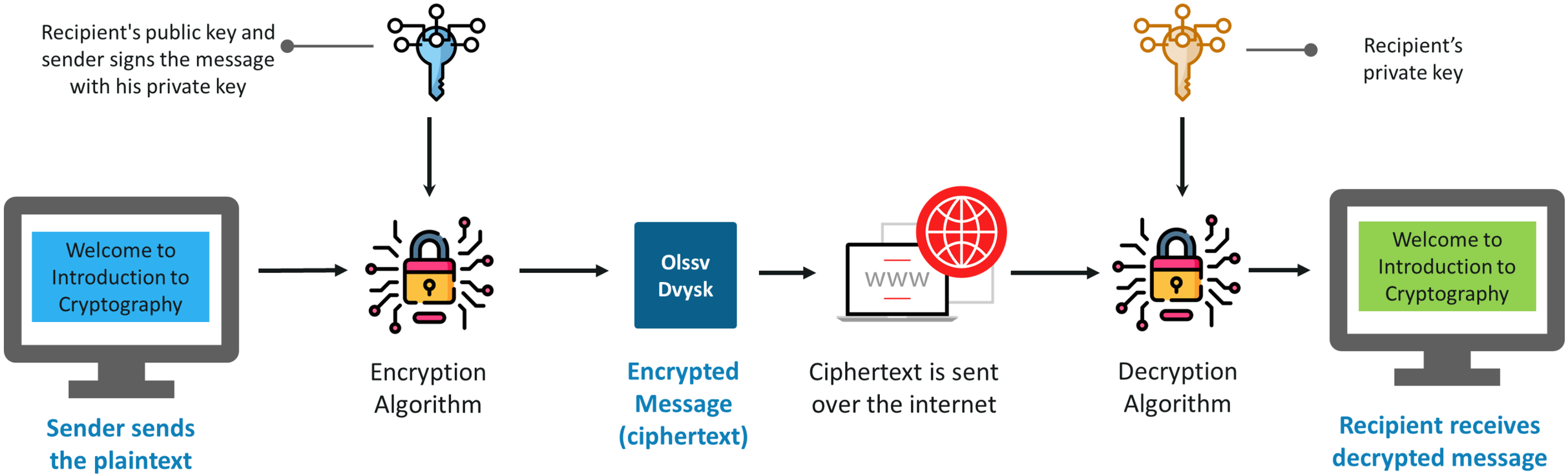
- **Authentication and Non Repudiation**
- message is encrypted with sender's private key ~ Authenticity

Asymmetric Cryptography—Services



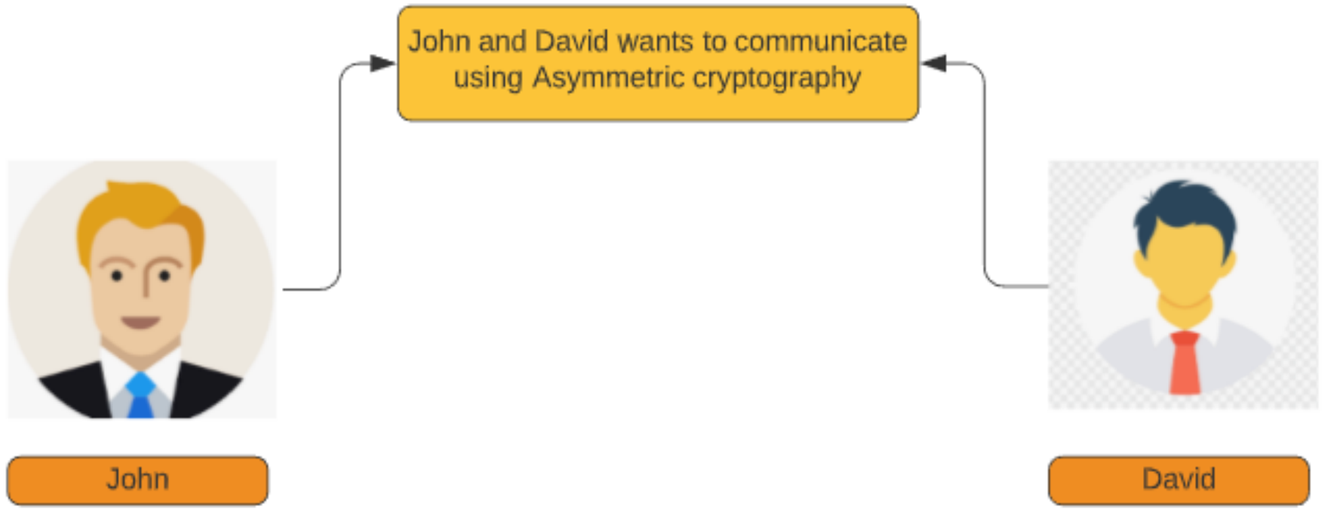


Introduction to Asymmetric Cryptography—Diagram



Secure Message Format-Confidentiality-Step 1

John and David Wants to communicate using Asymmetric cryptography



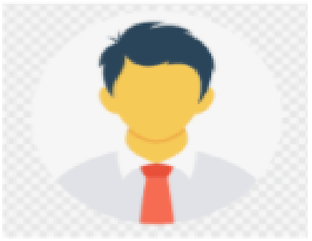
Secure Message Format-Confidentiality-Step 2

John and David generates Private key and Public key at their individual systems respectively

John generates Private key and Public key

John

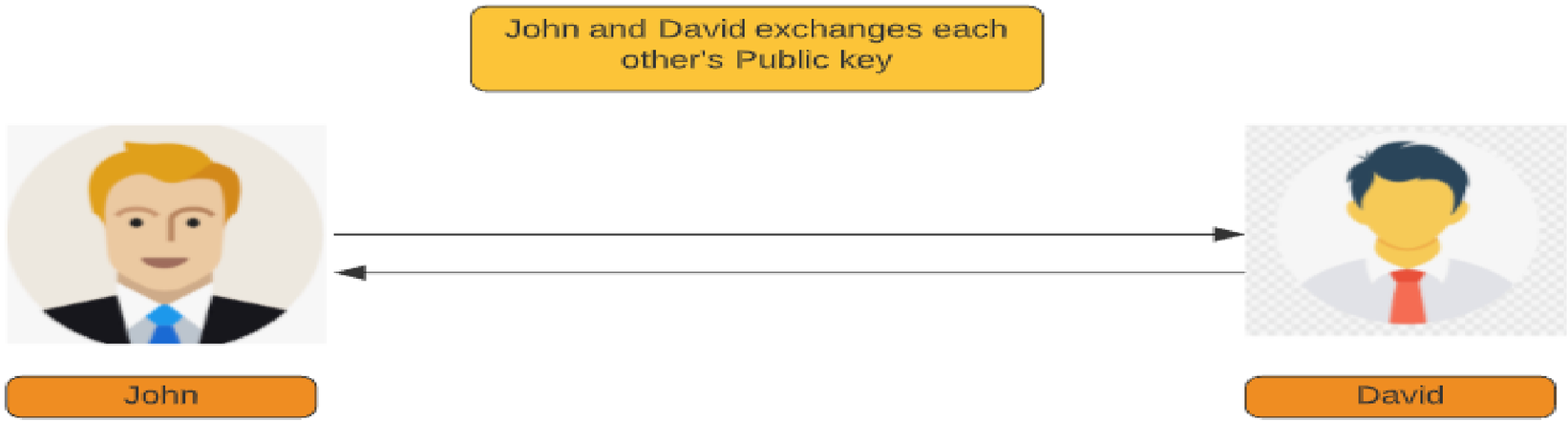
David generates Private key and Public key



David

Secure Message Format-Confidentiality-Step 3

John and David exchanges each other public key

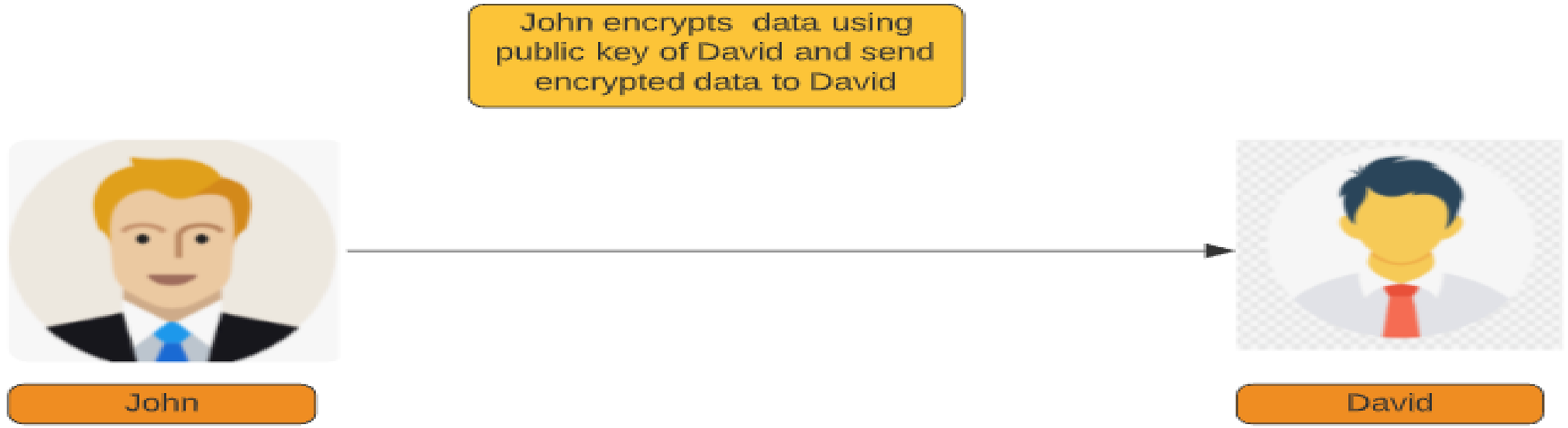


Secure Message Format-Confidentiality-Step 4

For achieving Secure Message Format(Confidentiality) , encrypt the data using Public key of Receiver(David).

If data is encrypted using receiver's(David) Public key, then it can only decrypted by receiver's(David) private key.

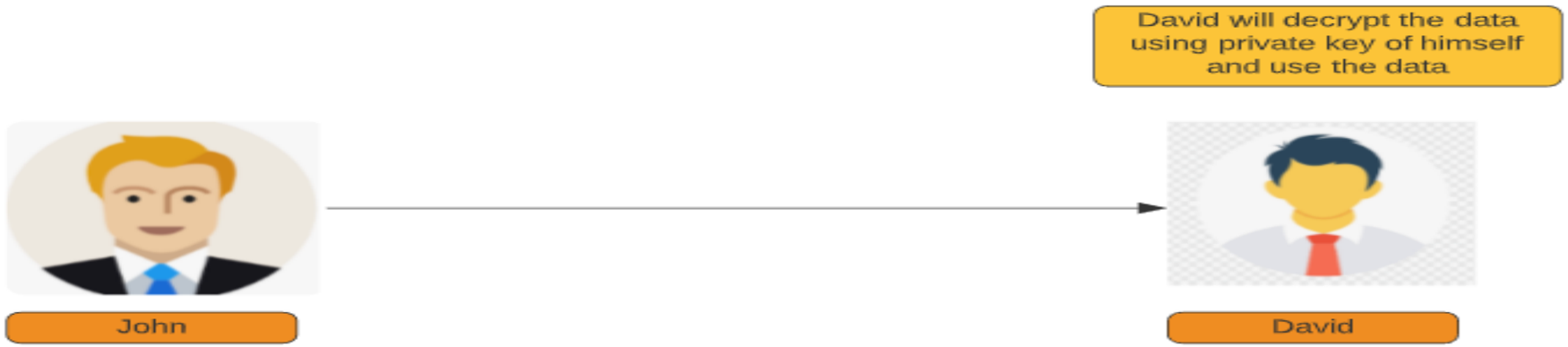
No one can decrypt in between as it needs receivers private key for decryption.



Secure Message Format-Confidentiality-Step 5

As data is encrypted using David's Public key, David can only decrypt data with his private key.

On receiving encrypted data, David uses his private key to decrypt data which ensures confidentiality.



Asymmetric Cryptography—Secure Message Format- Summarized View

Step 1
- User A and B wants to communicate using Asymmetric Cryptography

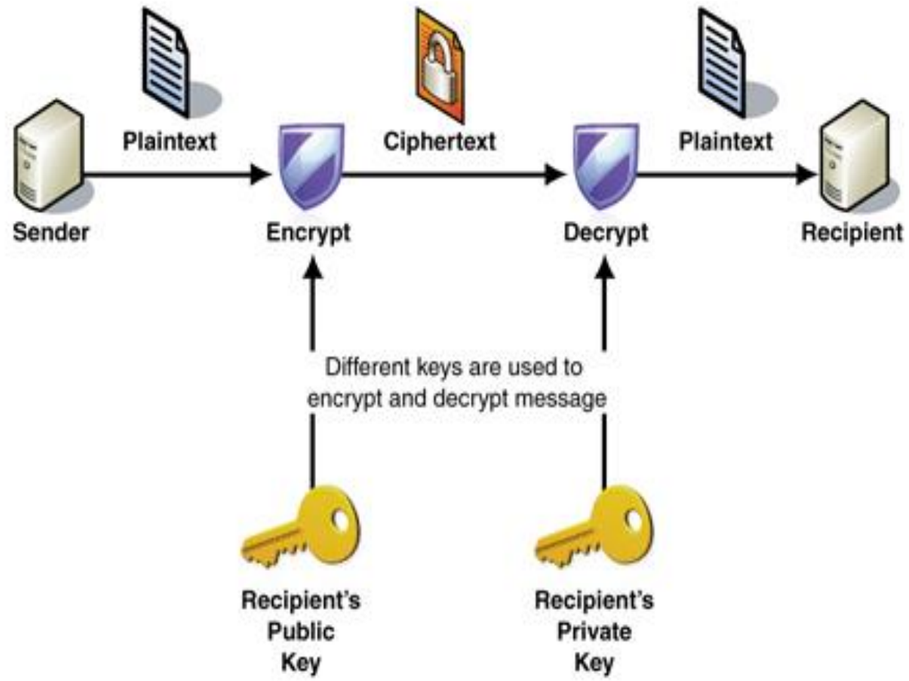
Step 2
- User A will generate Private Key and Public Key at its system

Step 3
- User B will generate Private Key and Public Key at its system

Step 4
- User A and User B exchanges each others public key.

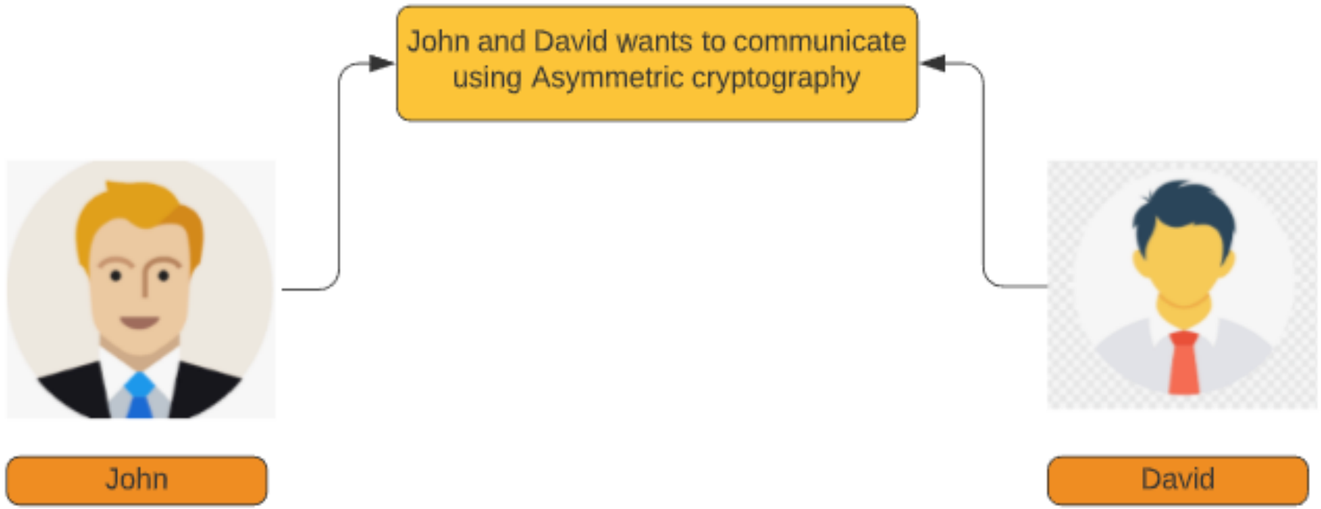
Step 5
- User A will encrypt data using public key of B and and send it to B

Step 6
- User B will use its private key to decrypt data which ensure confidentiality



Open Message Format-Authentication-Step 1

John and David Wants to communicate using Asymmetric cryptography



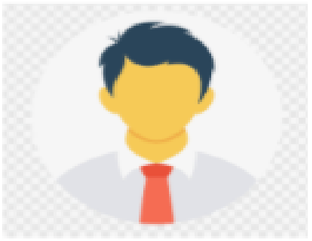
Open Message Format-Authentication-Step 2

John and David generates Private key and Public key at their individual systems respectively

John generates Private key and Public key

John

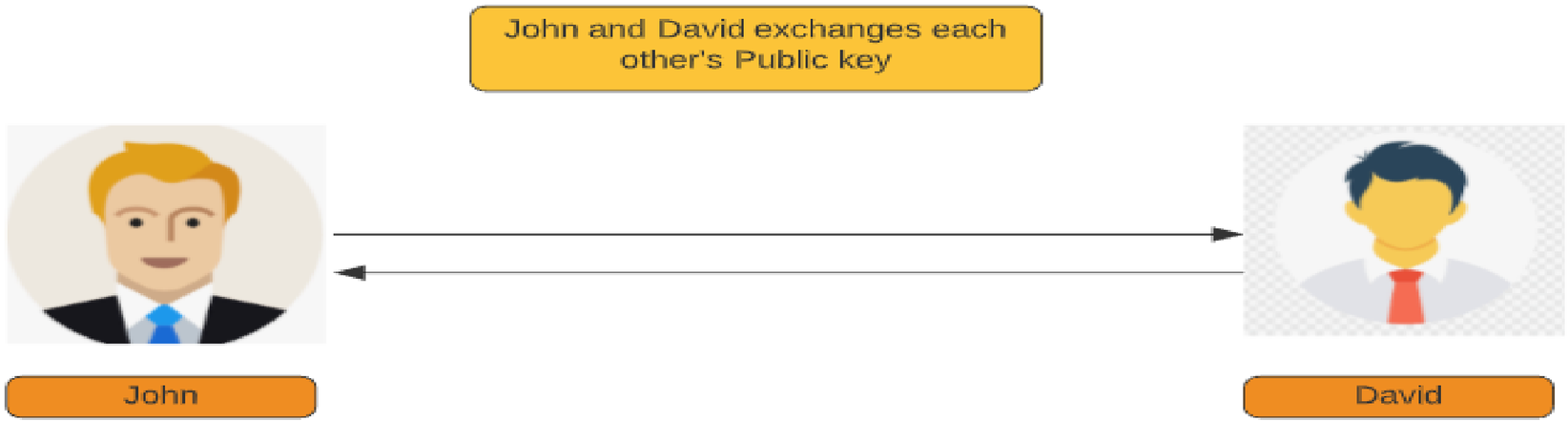
David generates Private key and Public key



David

Open Message Format-Authentication-Step 3

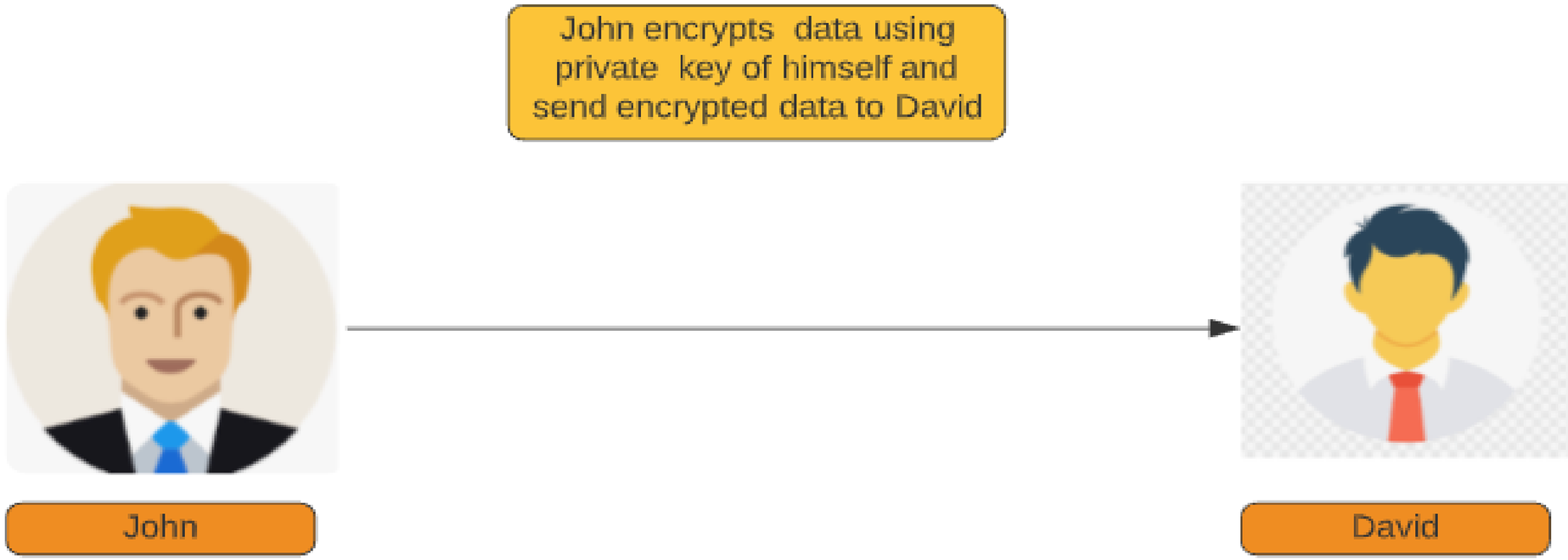
John and David exchanges each other public key



Open Message Format-Authentication-Step 4

For achieving Open Message Format(Authentication) , encrypt the data using Private key of Sender (John).

If data is encrypted using Sender's (John) Private key, then it can only be decrypted by Sender's (John) Public key.

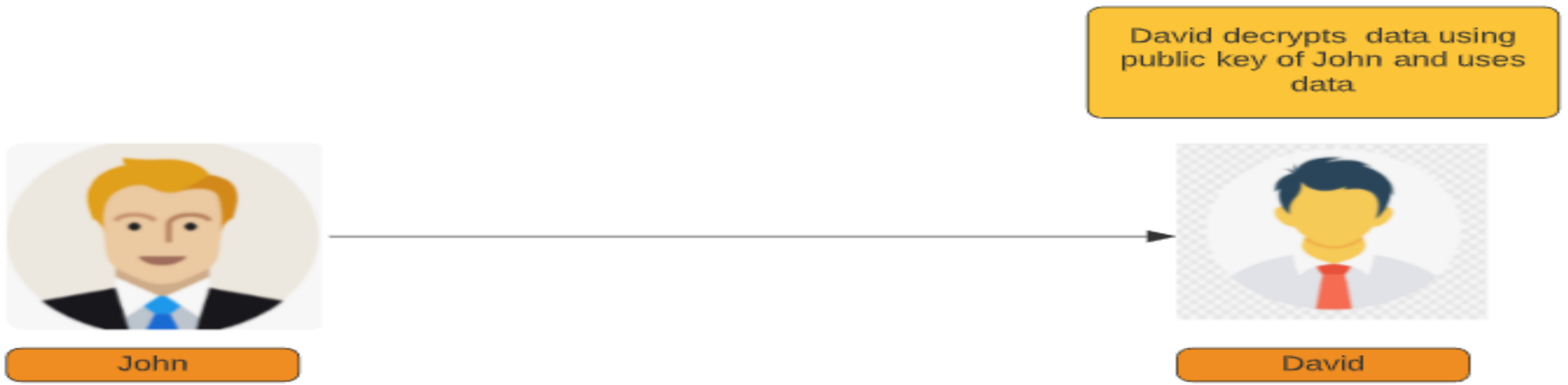


Open Message Format-Authentication-Step 5

As data is encrypted using private key of John, this can only be decrypted using Public key of John.

David will decrypt data using public key of John and start using it.

As this can be decrypted using private key of sender(John), so anyone with John' s Public key can open it, hence no confidentiality and that is why it is called open message format



Asymmetric Cryptography—Open Message Format- Authentication and Non Repudiation-Summarized view

Step 1
- User A and B wants to communicate using Asymmetric Cryptography

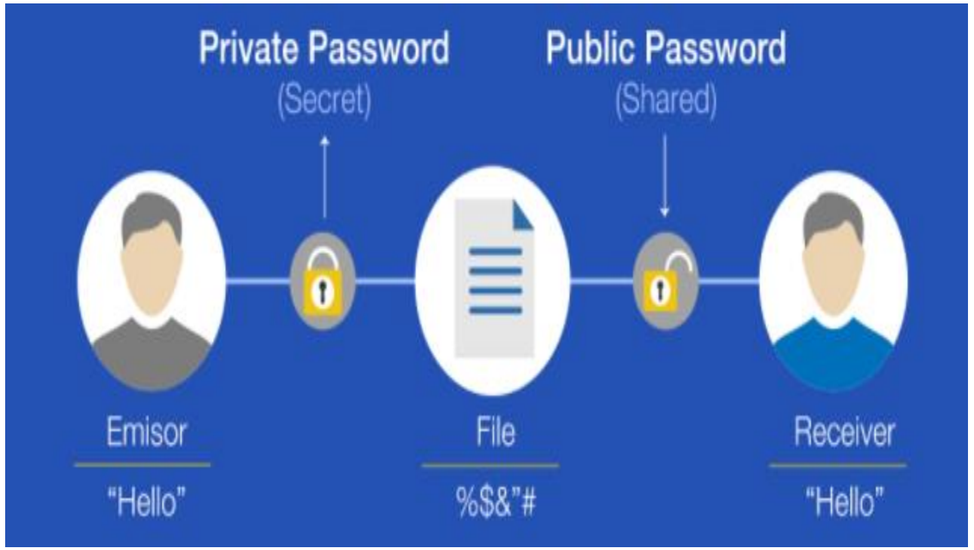
Step 2
- User A will generate Private Key and Public Key at its system.

Step 3
- User B will generate Private Key and Public Key at its system

Step 4
- User A and User B exchanges each others public key

Step 5
- User A will encrypt data using private key of A and send it to B

Step 6
- User B will use Public key of A to decrypt data which ensure Authentication and Non Repudiation



Types of Asymmetric Cryptography

RSA:

- RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of this algorithm.
- Is a worldwide de facto standard
- Provides digital signatures, encryption, and secret key distribution
- Is based on the difficulty in factoring the two large prime number's (up to 200 digits long) product forms
- Used in Web browsers with SSL, systems that use public key cryptosystems

Elliptic Curve Cryptosystems (ECCs)

- Instead of generating keys as the product of very large prime numbers, ECC generates keys through the properties of the elliptic curve equation.
- An ECC key of 160-bit provides the same protection as a 1024-bit RSA key.
- ECC is more efficient than RSA
- Provides encryption, digital signature, key exchange
- Used in devices with limited processing, storage and bandwidth capacity ie Wireless and mobile phone.

El Gamal

- It leverages Diffie-Hallman algorithm for encryption and decryption
- Major disadvantage—the algorithm doubles the length of any message it encrypts

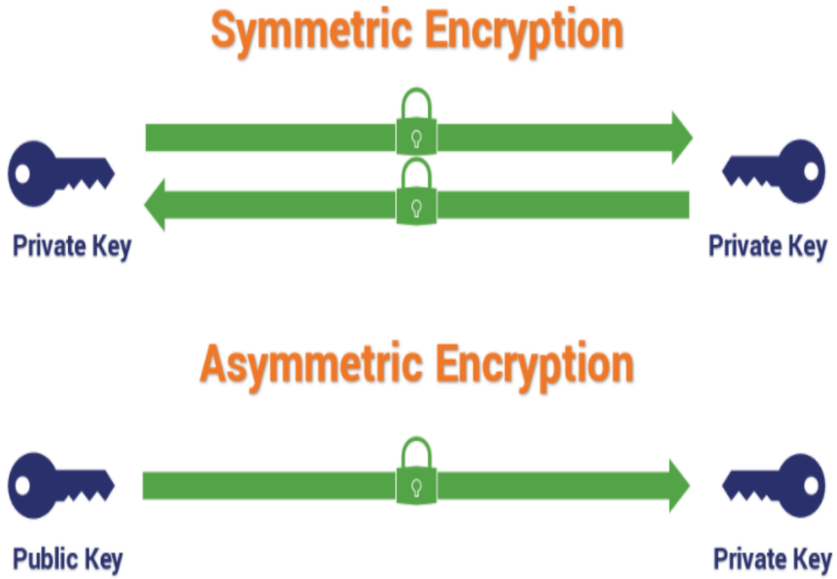
Symmetric vs. Asymmetric Cryptography

Symmetric Cryptography

- Same key is used for encryption and decryption in symmetric algorithms
- Symmetric algorithms consume less computing power.
- Symmetric algorithms are much faster.
- “Symmetric key” is synonymous with secret key or session key

Asymmetric Cryptography

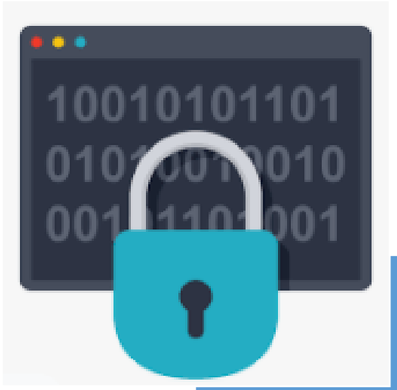
- A pair of keys, one for encryption and the other for decryption, are used in asymmetric algorithms
- Asymmetric algorithms consume more computing power
- Asymmetric algorithms are used to distribute the symmetric key as they are slower.
- In an asymmetric algorithm the encryption key is called public key and decryption key is called private or secret key and the “asymmetric key” refers to the public key or private key of an asymmetric key pair



Advantages and Disadvantages

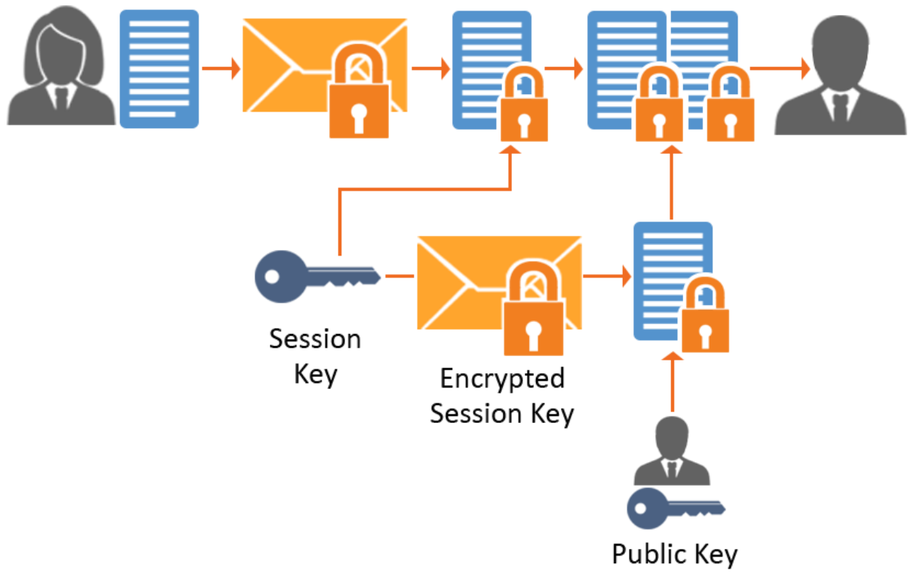
Types of cryptography	Advantages	Disadvantages
Symmetric Cryptography	• Very fast to encrypt or decrypt, secure, and affordable • Best for encrypting large files	• Presents the challenge of key management • Does not provide authenticity, non-repudiation
Asymmetric Cryptography	• Provides better key distribution than symmetric systems • Provides better scalability due to ease of key distribution • Provides authenticity and non-repudiation, in addition to confidentiality .	• Much slower operation than symmetric systems • Vulnerable to man-in-the-middle attacks

Hybrid Key Cryptography or Digital Envelope



Hybrid key Cryptography

- A hybrid system that combines the symmetric and asymmetric methods.
- The more efficient symmetric algorithm encrypts a message using a secret key.
- The symmetric secret key is encrypted using recipient's public key with an asymmetric algorithm.
- The message encrypted with that secret key and the encrypted symmetric secret key are sent to the recipient.
- The recipient uses his private key to decrypt the secret key.
- The secret key is then used to decrypt the message.
- A symmetric algorithm is used for bulk encryption.
- To distribute the symmetric key the asymmetric algorithm is used.



Hybrid Cryptography-Digital Envelope

Step 1
- A generates symmetric key and it encrypt bulk data using symmetric key

Step 2
- User A wants to send symmetric key and encrypted data in secure manner to B

Step 3
- User A will use Asymmetric key cryptography to send symmetric key in secure manner to B

Step 4
- User A will generate Private Key and Public Key at its system

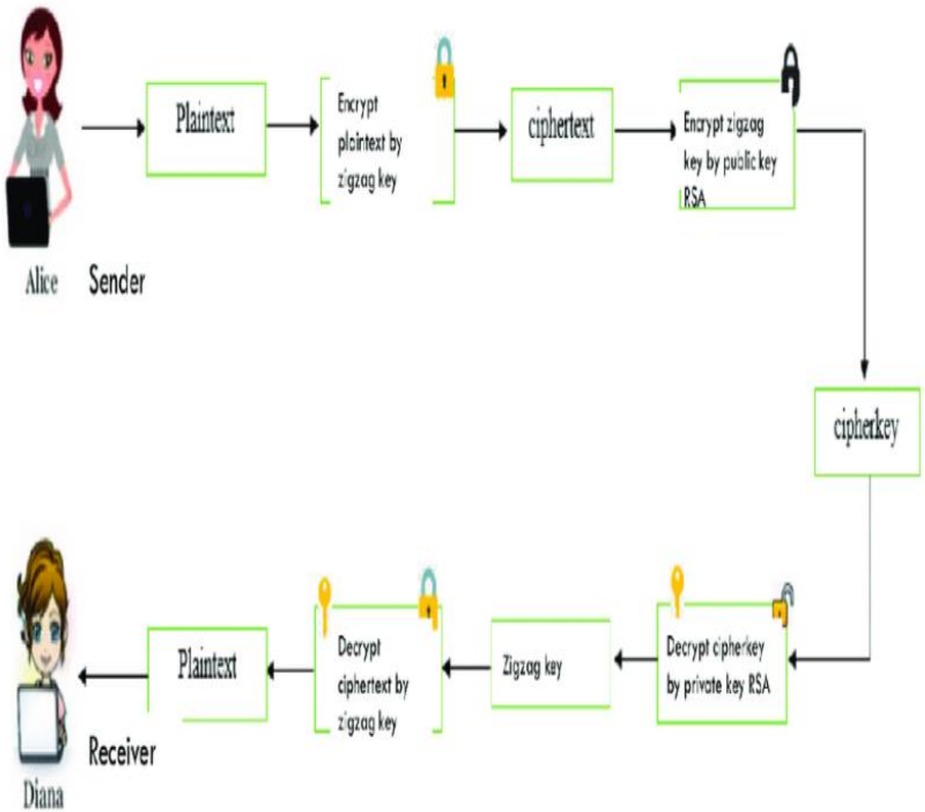
Step 5
- User B will generate Private Key and Public Key at its system

Step 6
- User A and User B exchanges each others public key

Step 7
- User A encrypt Symmetric key which was used for encrypting Bulk data in step 1 with Public key of B and send encrypted data and encrypted symmetric key

Step 8
- User B decrypt symmetric key using private key of itself

Step 9
- User B will decrypt bulk data using symmetric key which is decrypted in step 7



SSL/TLS

Step 1

- Client Browser requests TLS/SSL session from Server

Step 2

- TLS certificate and Public key of Server is being sent to client .

Step 3

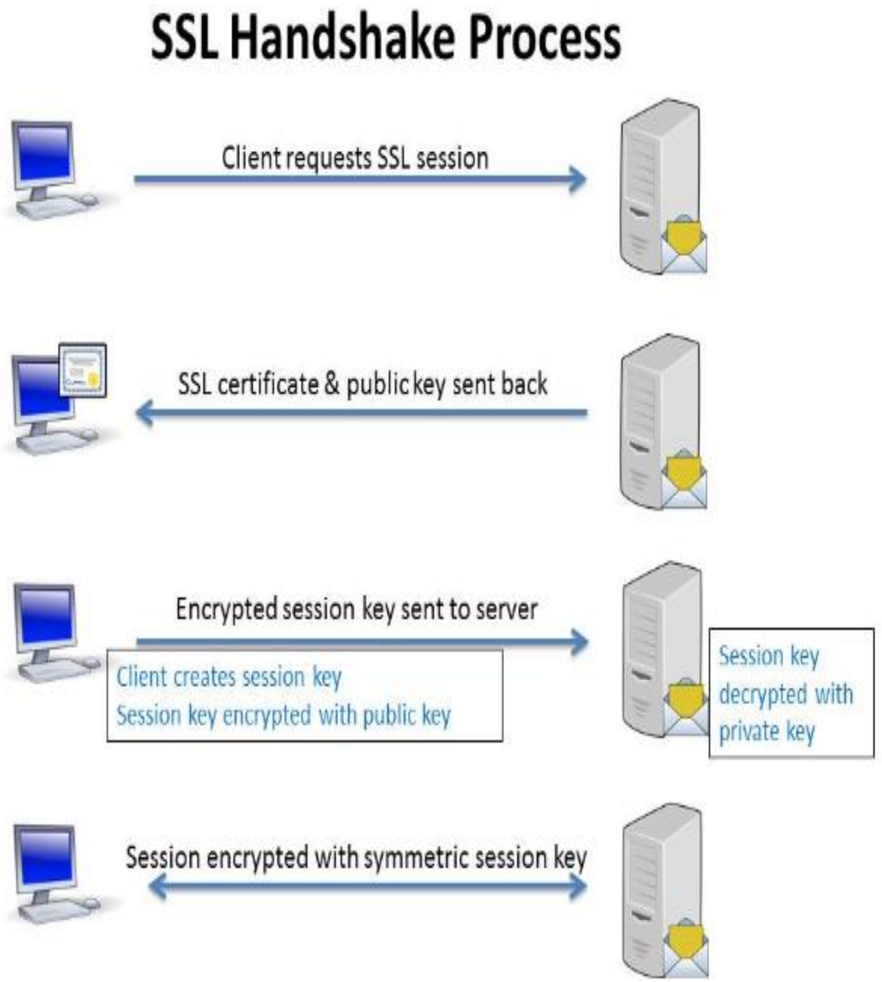
- Client generate Session key and encrypt this session key with server's public key and send to server.

Step 4

- Server on receiving encrypted session key , perform the decryption process with its private key.

Step 5

- Client now send the data encrypted with session key and server already have a session key whih it uses to decrypt the actual data.



Thank You