TRIAD
SQUARE INFOSEC PVT.LTD

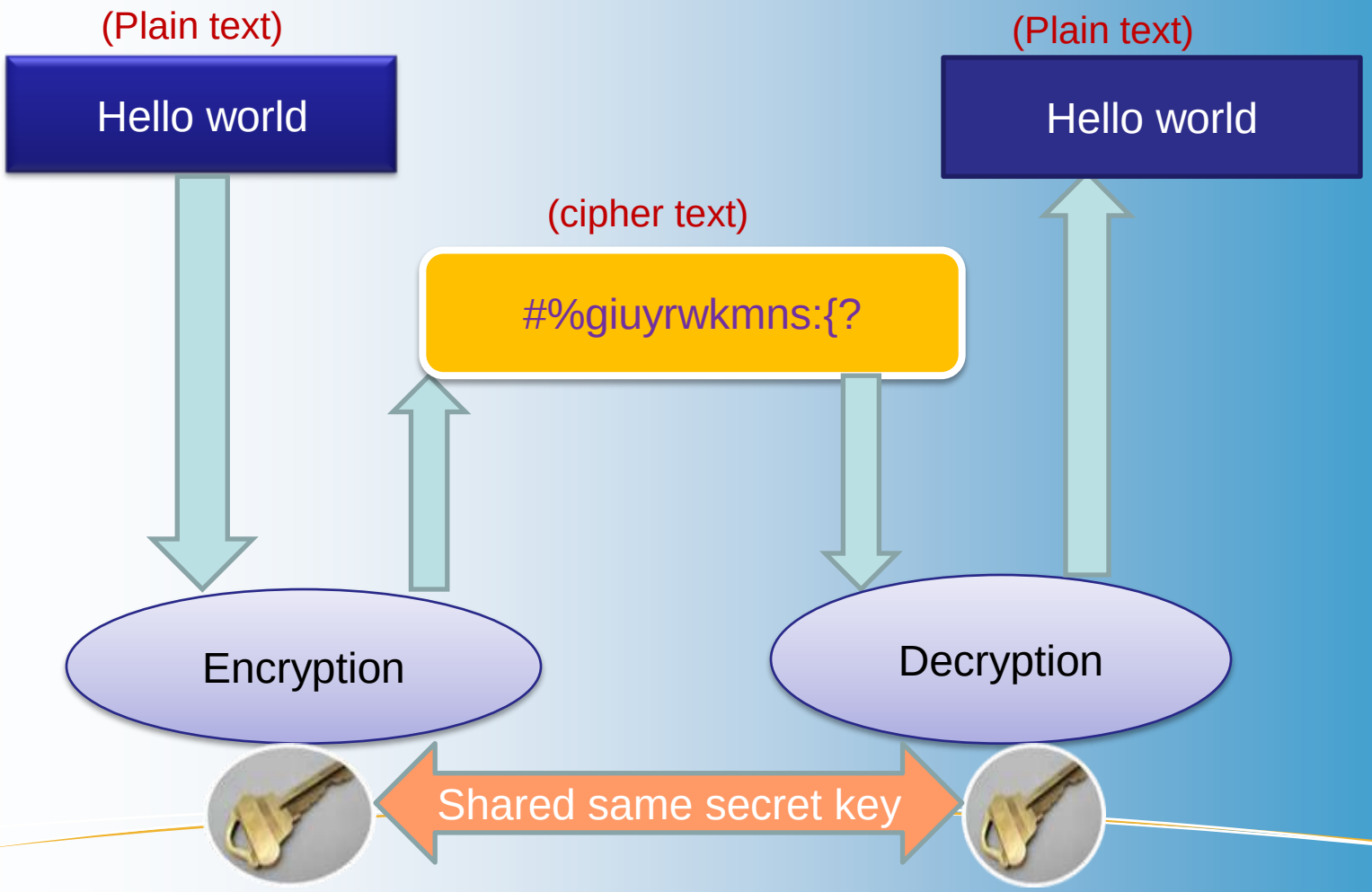
Symmetric & Asymmetric encryption

SYMMETRIC ENCRYPTION

TRIAD
SQUARE INFOSEC PVT.LTD

- An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
- In other terms, Data is encrypted and decrypted using the same key.
- Symmetric-key cryptography is sometimes called *secret-key cryptography.*

SYMMETRIC ENCRYPTION (cont..)



SYMMETRIC ENCRYPTION (cont..)

TRIAD
SQUARE INFOSEC PVT.LTD

- Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted, Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.

- Examples of symmetric algorithms are DES, 3DES and AES

Symmetric Encryption Algorithms

TRIAD
SQUARE INFOSEC PVT.LTD

- The most popular symmetric-key system is the *Data Encryption Standard (DES)*.
- DES uses 56-bit keys, they are short enough to be easily brute-forced by modern hardware and it is recommended that DES should not to be used.
- Triple DES (or 3DES) uses 128 bits key length, the same algorithm, applied three times to produce strong encryption.

MERITS & DE-MERITS

TRIAD
SQUARE INFOSEC PVT.LTD

Merits:

- SIMPLER
- FASTER

De-Merits:

- Two parties must somehow exchange the key in a secure way.
- Public key is distributed in a non-secure way b/n Client/Server.
- Easy for hackers to get the key as it is shared in unsecure way.

ASYMMETRIC ENCRYPTION

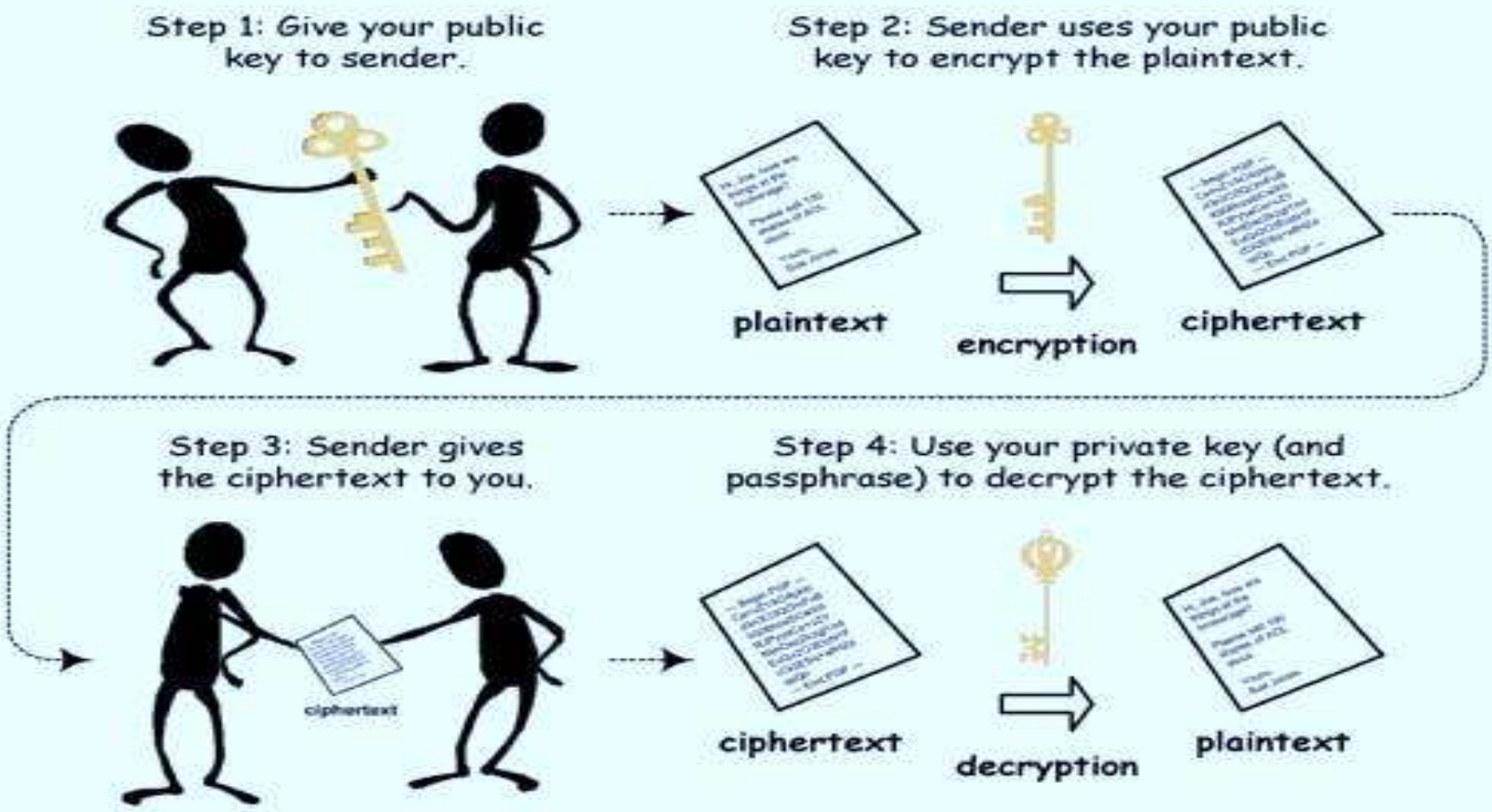
TRIAD
SQUARE INFOSEC PVT.LTD

Asymmetric encryption:

Asymmetric encryption use two keys, one to encrypt the data, and another key to decrypt the data. These keys are generated together. One is named as Public key and is distributed freely. The other is named as Private Key and it is kept hidden.

Both Sender & Recipient has to share their Public Keys for Encryption and has to use their Private Keys for Decryption.

How it WORKS…….?



Key Points in Asymmetric Encryption

TRIAD
SQUARE INFOSEC PVT.LTD

- Asymmetric encryption use two keys:

  Public Key - to encrypt the data

  Private Key - to decrypt the data

- These keys are generated together.
- The Public key(s) is distributed freely between the sender and receiver.
- The other is named as Private Key and it is kept hidden.
- The Private Key is only used for Decryption and will not be shared between the sender and receiver.

Asymmetric Encryption Algorithms

❖RSA: Rivest-Shamir-Adleman is the most commonly used asymmetric algorithm (public key algorithm). It can be used both for encryption and for digital signatures.

❖Digital Signature Algorithm: The standard defines DSS to use the SHA-1 hash function exclusively to compute message. The main problem with DSA is the fixed subgroup size (the order of the generator element), which limits the security to around only 80 bits. Hardware attacks can be menacing to some implementations of DSS. However, it is widely used and accepted as a good algorithm.

❖Diffie-Helman: Diffie-Hellman is the first asymmetric encryption algorithm, invented in 1976, using discrete logarithms in a finite field. Allows two users to exchange a secret key over an insecure medium without any prior secrets.

Asymmetric Encryption Algorithms

❖ElGamal: The ElGamal is a public key cipher - an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. ElGamal is the predecessor of DSA.

❖ECDSA: Elliptic Curve DSA (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups. As with Elliptic Curve Cryptography in general, the bit size of the public key believed to be need ECDSA is about twice the size of the security level, in bits.

❖XTR: It is based on the primitive underlying the very first public key cryptosystem, the Diffie-Hellman key agreement protocol. Some advantages of XTR are its fast key generation (much faster than RSA), small key sizes (much smaller than RSA, comparable with ECC for current security settings), and speed.

MERITS & DE-MERITS

TRIAD
SQUARE INFOSEC PVT.LTD

Merits:

❖ Two parties don't need to have their private keys already shared in order to communicate using encryption.

❖ Authentication and Non-Repudiation are possible. (Authentication means that you can encrypt the message with my public key and only I can decrypt it with my private key. Non-repudiation means that you can "sign" the message with your private key and I can verify that it came from you with your public key.)

De-Merits:

❖Asymmetric Encryption algorithms are comparatively complex.

❖Time consuming process for Encryption and Decryption.