StaySecure

8

2019

Your monthly dose of cyber security

Topic: Symmetric Cryptography

What is Symmetric Cryptography?

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used for both encrypting and decrypting messages. It is essential that, without this key, the message cannot be decrypted and, at the same time, that the algorithm used (mostly public) is such that we can obtain the corresponding original text by using this key.

Advantages

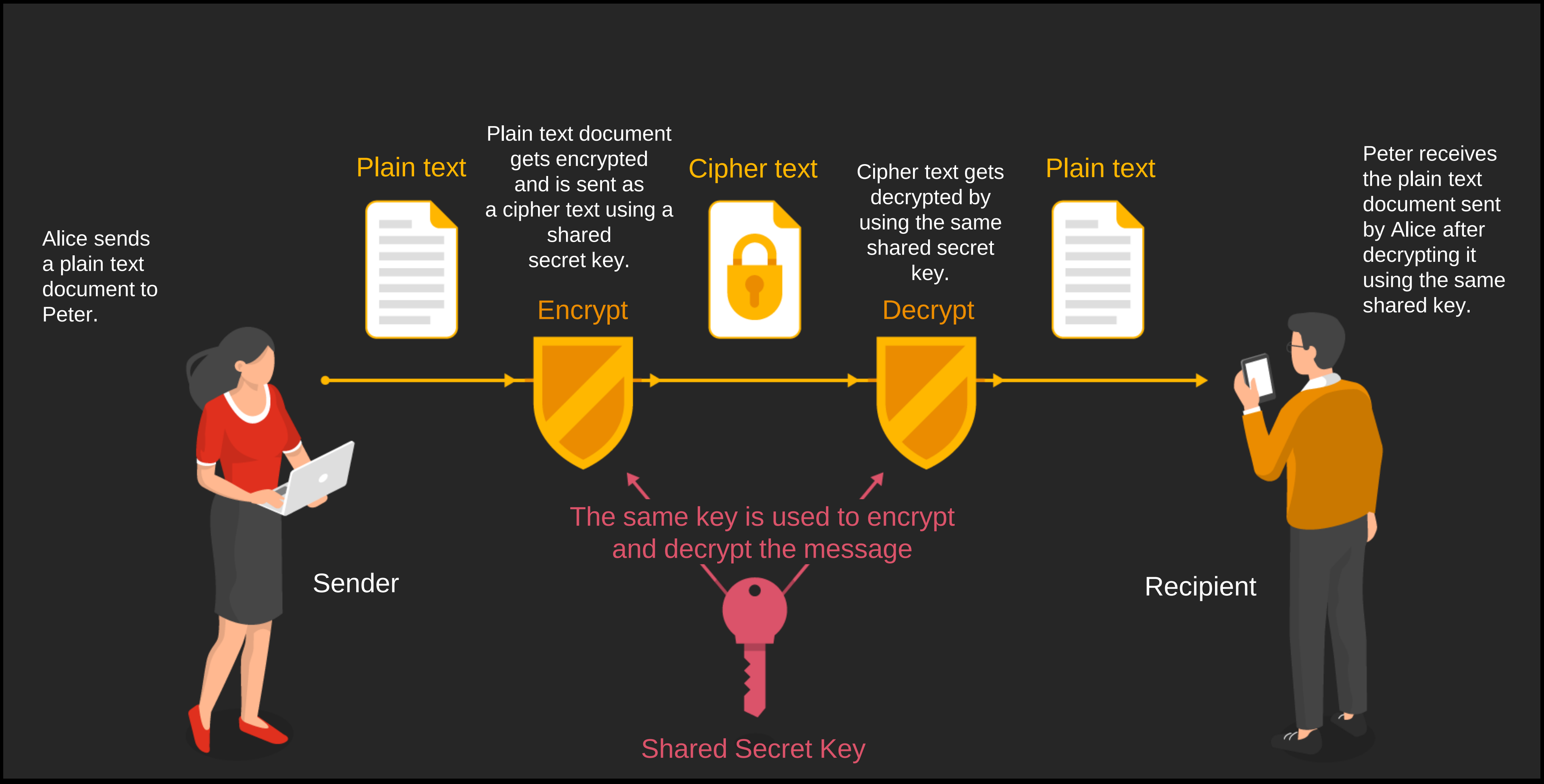
✓ Easy implementation and fast encryption of a huge amount of data by using short keys for symmetric ciphers

✓ Basis for creating various cryptographic mechanisms with the possibility to combine ciphers to create much stronger ones

Disadvantages

✓ Parties need to share the key with each other, what can lead the key being revealed and so allowing attacker to crack the algorithm

✓ Necessity to keep a large number of encryption keys and change them frequently to ensure secure communication



Alice sends a plain text document to Peter.

Plain text document gets encrypted and is sent as a cipher text using a shared secret key.

Cipher text gets decrypted by using the same shared secret key.

Peter receives the plain text document sent by Alice after decrypting it using the same shared key.

The same key is used to encrypt and decrypt the message

Is it possible to hack it? Yes, it is.

To crack this system, an attacker needs to uncover the secret key and the algorithm. These two elements prevent decryption of the text in communication. Transmission of keys over an unsecured network can lead to unauthorized access to the symmetric key and consequent data misuse by the attacker. The attacker uses the field cryptanalysis, which is a process for finding weaknesses in cryptographic algorithms and using these weaknesses to decipher the cipher text without knowing the secret key (instance deduction).

How we can help you?

If you are interested in encryption and have other questions, do not hesitate to contact me. I would be happy to advise you in other areas of cyber defense and I am ready to provide immediate help.

IT Security department