Entry Level Cybersecurity Interview Questions

By Surendra Pander {@technical surendra}

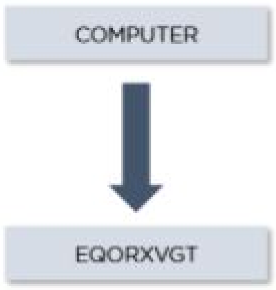
Cyber Security Interview Questions - Cryptography

This section of cyber security interview questions is based on the concept of cryptography.

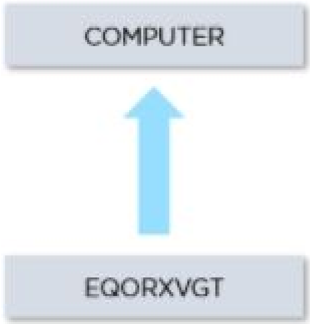
75. Define cryptography, encryption, and decryption.

Ethical hackers use cryptography to secure information. It involves converting data from a readable format to a non-readable format and vice versa.

Encryption: Converting a message from a readable state to a scrambled state, making no sense. In the below example, Key = Alphabet + 2.

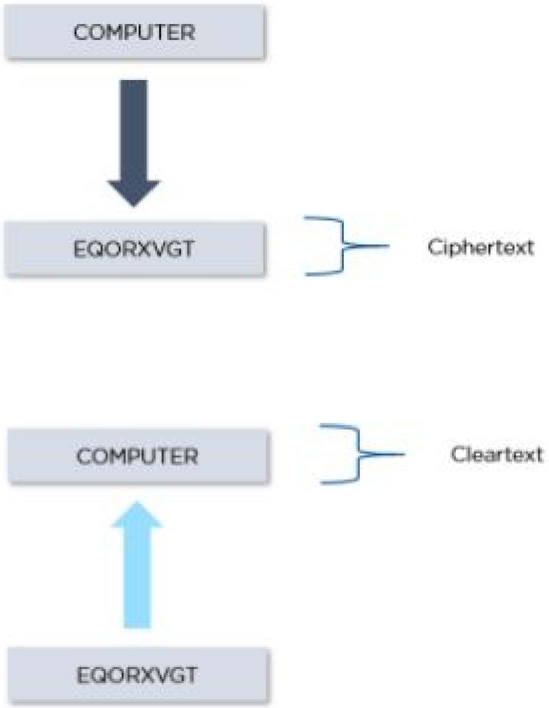


Decryption: The message is decrypted using a secret key that is known only to the recipient. Decryption = Alphabet - 2 in the given example.



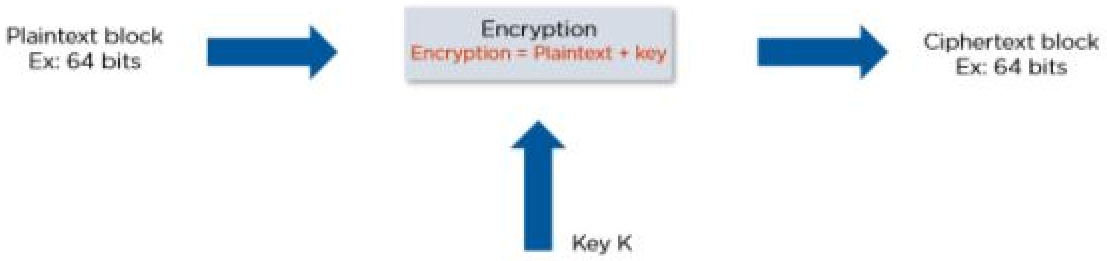
76. What is the difference between ciphertext and cleartext?

Ciphertext refers to the text which is encrypted and undecipherable. The message received after decryption is known as cleartext. This text is understandable.



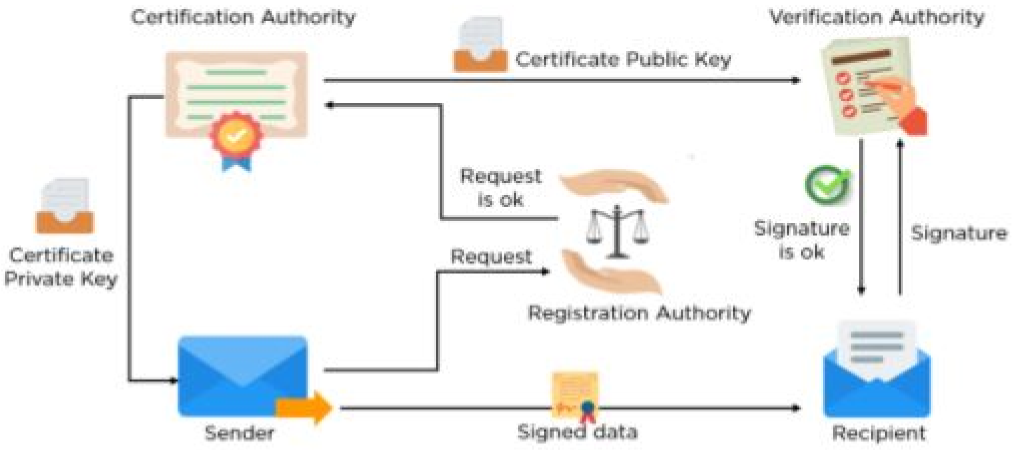
77. What is a block cipher?

This refers to the method of encrypting the plain message block by block. The plain message is broken down into fixed-size blocks and then encrypted.



78. What is Public Key Infrastructure?

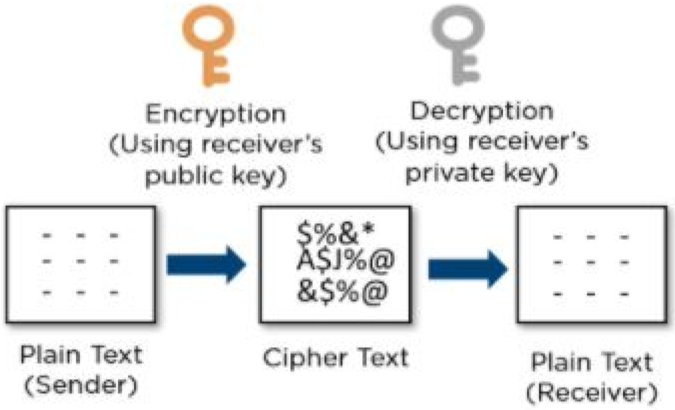
Public Key Infrastructure (PKI) is a set of policies that secures the communication between a server and a client. It uses two cryptographic keys, public and private.



PKI enables trusted digital identities for people. PKI grants secure access to digital resources. The core of PKI is a certificate authority, which ensures the trustworthiness of the digital data.

79. What is RSA?

RSA is a public-key cryptosystem that is used for secure data transmission. RSA stands for Rivest, Shamir, and Adleman, who are the inventors of the technique. It is an asymmetric cryptography algorithm that works on both public and private keys. Here, the encryption key is public, and the decryption key is kept private.



80. What are a few of the alternatives to RSA?

The alternatives to RSA are as follows:

1. Duo Security
2. Okta
3. Google Authenticator
4. LastPass

81. What are the prime objectives of modern cryptography?

The prime objectives of modern cryptography are:

1. Confidentiality: Confidentiality helps in keeping the information safe from unauthorized people.
2. Non-repudiation: Non-repudiation prevents denial in an electronic transaction.
3. Authenticity: Authenticity helps in identifying the source of the created information.
4. Integrity: Integrity makes sure that the data received by the receiver is not modified.

82. What is SAFER?

Secure and Fast Encryption Routine(SAFER) is a block cipher. This has a 64-bit block size and a byte-oriented algorithm. SAFER's encryption and decryption procedures are highly secure. This technology is used widely in applications like digital payment cards.

83. How does the Public Key Infrastructure (PKI) work?

The working of Public Key Infrastructure (PKI) at a macro level is as follows:

1. Firstly, the request for the Digital Certificate is sent to the appropriate CA (Certificate Authority).
2. Once the request is processed, the Digital Certificate is issued to the person requesting it.
3. After that, the Digital Certificate gets signed by confirming the identity of the person.
4. Now, the Digital Certificate can be used to encrypt the cleartext into a ciphertext, which is sent from the sending party to the other party.

84. What is the Blowfish algorithm?

It is a 64-bit symmetric encryption algorithm. The same secret key is used for encrypting and decrypting. Here, the operations are based on exclusive ors and additions on 32bit words. The key has a maximum length of 448 bits; it is variable. It is also used to generate several subkey arrays.

My social medial accounts -

Twitter — https://twitter.com/technicalSure

YouTube — https://www.youtube.com/channel/UCZq87M0I0-zEfLuyyfEeE6Q

Instagram — https://www.instagram.com/surendra_choudhary1241/

Linkedin — https://www.linkedin.com/in/surendra-pander-4066761b7/