# Encryption Decryption Interview Questions And Answers Guide.

**Global Guideline.**

**https://globalguideline.com/**

# Encryption Decryption Job Interview Preparation Guide.



**Question # 1**

What is Public-Key Cryptography?

**Answer:-**

Traditional cryptography is based on the sender and receiver of a message knowing and using the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is known as secret-key or symmetric cryptography. The main problem is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, or a phone system, or some other transmission medium to prevent the disclosure of the secret key being communicated. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys is called key management; all cryptosystems must deal with key management issues. Because all keys in a secret-key cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users.

Read More Answers.

**Question # 2**

What are the CFB and OFB modes?

**Answer:-**

The Cipher Feedback (CFB) mode and the Output Feedback (OFB) mode are two more standard modes of operation for a block cipher.
In CFB mode, the previous ciphertext block is encrypted and the output produced is combined with the plaintext block using exclusive-or to produce the current ciphertext block. It is possible to define CFB mode so that it uses feedback that is less than one full data block. An initialization vector or value c0 is used as a "seed" for the process.

Read More Answers.

**Question # 3**

What is the ElGamal Cryptosystem?

**Answer:-**

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

Read More Answers.

**Question # 4**

What is the McEliece Cryptosystem?

**Answer:-**

The McEliece cryptosystem is a public-key encryption algorithm based on algebraic coding theory. The system uses a class of error-correcting codes, known as the Goppa codes, for which fast decoding algorithms exist. The basic idea is to construct a Goppa code as the private key and disguise it as a general linear code, which is the public key. The general linear code cannot be easily decoded unless the corresponding private matrix is known.

Read More Answers.

**Question # 5**

What is Multiple Encryption?

**Answer:-**

Intuitively, we might expect that by encrypting a message twice with some block cipher, either with the same key or by using two different keys, then we would expect the resultant encryption to be stronger in all but some exceptional circumstances. And by using three encryptions, we would expect to achieve a yet greater level of security. While there are some more complicated issues to consider, this is pretty much the case, and triple-DES has been used for a considerable time as a more secure cipher for protecting the keys used with single-DES. However, there are some surprising results when we consider exactly how much additional protection is provided by using double and triple encryption.

Read More Answers.

**Question # 6**

What are the Advantages and Disadvantages of Public-Key Cryptography Compared with Secret-Key Cryptography?

**Answer:-**

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel), and there may be a chance that an enemy can discover the secret keys during their transmission.
Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos secret-key authentication system involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. Public-key authentication, on the other hand, prevents this type of repudiation; each user has sole responsibility for protecting his or her private key. This property of public-key authentication is often called non-repudiation.

Read More Answers.

**Question # 7**

How is RSA used for Encryption in Practice?

**Answer:-**

RSA is combined with a secret-key cryptosystem, such as DES, to encrypt a message by means of an RSA digital envelope.
Suppose Alice wishes to send an encrypted message to Bob. She first encrypts the message with DES, using a randomly chosen DES key. Then she looks up Bob's public key and uses it to encrypt the DES key. The DES-encrypted message and the RSA-encrypted DES key together form the RSA digital envelope and are sent to Bob. Upon receiving the digital envelope, Bob decrypts the DES key with his private key, then uses the DES key to decrypt to message itself. This combines the high speed of DES with the key-management convenience of RSA.

Read More Answers.

**Question # 8**

What are the ECB and CBC Modes?

**Answer:-**

When we use a block cipher to encrypt a message of arbitrary length, we use techniques that are known as modes of operation for the block cipher. Modes must be at least as secure and as efficient as the underlying cipher. Modes may have properties in addition to those inherent in the basic cipher. The standard DES modes have been published in FIPS PUB 81 and as ANSI X3.106. A more general version of the standard generalized the four modes of DES to be applicable to a block cipher of any block size. The standard modes are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB).

Read More Answers.

**Question # 9**

What are the Counter and PCBC Modes?

**Answer:-**

Due to shortcomings in OFB mode Diffie has proposed an additional mode of operation, termed the counter mode. It differs from OFB mode in the way the successive data blocks are generated for subsequent encryptions. Instead of deriving one data block as the encryption of the previous data block, Diffie proposed encrypting the quantity i + IV (mod 264) for the ith data block, where IV is some initialization vector.

Read More Answers.

**Question # 10**

What is a One-Way Function?

**Answer:-**

A one-way function is a mathematical function that is significantly easier to perform in one direction (the forward direction) than in the opposite direction (the inverse direction). It might be possible, for example, to compute the function in seconds but to compute its inverse could take months or years. A trap-door one-way function is a one-way function where the inverse direction is easy given a certain piece of information (the trap door), but difficult otherwise.

Read More Answers.

**Question # 11**

What are Elliptic Curve Cryptosystems?

**Answer:-**

Elliptic curve cryptosystems are analogs of public-key cryptosystems such as RSA and ElGamal, in which modular multiplication is replaced by the elliptic curve addition operation.
The curves used in elliptic curve analogs of discrete logarithm cryptosystems are normally of the form
$y2 = x3 + ax + b \pmod p$,
where p is prime. The problem tapped by the discrete logarithm analogs in elliptic curves is the elliptic curve logarithm problem, defined as follows: given a point G on an elliptic curve with order r (number of points on the curve) and another point Y on the curve, find a unique x (0 x r - 1) such that Y = xG, i.e., Y is the xth multiple of G.

Read More Answers.

**Question # 12**

What is Probabilistic Encryption?

**Answer:-**

Probabilistic encryption, discovered by Goldwasser and Micali [GM84], is a design approach for encryption where a message is encrypted into one of many possible ciphertexts (not just a single ciphertext as in deterministic encryption), in such a way that it is provably as hard to obtain partial information about the message from the ciphertext, as it is to solve some hard problem. In previous approaches to encryption, even though it was not always known whether one could obtain such partial information, neither was it proved that one could not do so.

Read More Answers.

**Question # 13**

What is the Significance of One-Way Functions for Cryptography?

**Answer:-**

Public-key cryptosystems are based on (presumed) trap-door one-way functions. The public key gives information about the particular instance of the function; the private key gives information about the trap door. Whoever knows the trap door can perform the function easily in both directions, but anyone lacking the trap door can perform the function only in the forward direction. The forward direction is used for encryption and signature verification; the inverse direction is used for decryption and signature generation.
In almost all public-key systems, the size of the key corresponds to the size of the inputs to the one-way function; the larger the key, the greater the difference between the efforts necessary to compute the function in the forward and inverse directions (for someone lacking the trap door). For a digital signature to be secure for years, for example, it is necessary to use a trap-door one-way function with inputs large enough that someone without the trap door would need many years to compute the inverse function.

Read More Answers.

**Question # 14**

What is LUC?

**Answer:-**

LUC is a public-key cryptosystem developed by a group of researchers in Australia and New Zealand. The cipher implements the analogs of ElGamal, Diffie-Hellman, and RSA over Lucas sequences. LUCELG is the Lucas sequence analog of ElGamal, while LUCDIF and LUCRSA are the Diffie-Hellman and RSA analogs. Lucas sequences used in the cryptosystem are the general second-order linear recurrence relation defined by

Read More Answers.

**Question # 15**

What is Merkles Tree Signature Scheme?

**Answer:-**

Merkle proposed a digital signature scheme that was based on both one-time signatures and a hash function and that provides an infinite tree of one-time signatures.
One-time signatures normally require the publishing of large amounts of data to authenticate many messages, since each signature can only be used once. Merkle's scheme solves the problem by implementing the signatures via a tree-like scheme. Each message to be signed corresponds a node in a tree, with each node consisting of the verification parameters that are used to sign a message and to authenticate the verification parameters of subsequent nodes. Although the number of messages that can be signed is limited by the size of the tree, the tree can be made arbitrarily large. Merkle's signature scheme is fairly efficient, since it requires only the application of hash functions.

Read More Answers.

**Question # 16**

What is the Rabin Signature Scheme?

**Answer:-**

The Rabin signature scheme is a variant of the RSA signature scheme. It has the advantage over RSA that finding the private key and forgery are both provably as hard as factoring. Verification is faster than signing, as with RSA signatures. In Rabin's scheme, the public key is an integer n where n = pq, and p and q are prime numbers which form the private key. The message to be signed must have a square root mod n; otherwise, it has to be modified slightly. Only about 1/4 of all possible messages have square roots mod n.

Read More Answers.

**Question # 17**

Do Digital Signatures Help Detect Altered Documents and Transmission Errors?

**Answer:-**

A digital signature is superior to a handwritten signature in that it attests to the contents of a message as well as to the identity of the signer. As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail. Thus, public-key authentication allows people to check the integrity of signed documents. If a signature verification fails, however, it will generally difficult to determine whether there was an attempted forgery or simply a transmission error.

Read More Answers.

**Question # 18**

What are Elliptic Curves?

**Answer:-**

Elliptic curves are mathematical constructions from number theory and algebraic geometry, which in recent years have found numerous applications in cryptography.
An elliptic curve can be defined over any field (e.g., real, rational, complex). However, elliptic curves used in cryptography are mainly defined over finite fields. An elliptic curve consists of elements (x, y) satisfying the equation
$y2 = x3 + ax + b$
together with a single element denoted O called the "point at infinity," which can be visualized as the point at the top and bottom of every vertical line. Addition of two points on a elliptic curve is defined according to a set of simple rules (e.g., point p1 plus point p2 is equal to point -p3 in Figure 2). The addition operation in an elliptic curve is the counterpart to modular multiplication in common public-key cryptosystems, and multiple addition is the counterpart to modular exponentiation.

Read More Answers.

**Question # 19**

What are Knapsack Cryptosystems?

**Answer:-**

The Merkle-Hellman knapsack cryptosystem is a public-key cryptosystem that was first published in 1978. It is commonly referred to as the knapsack cryptosystem. It is based on the subset sum problem in combinatorics. The problem involves selecting a number of objects with given weights from a large set such that the sum of

the weights is equal to a pre-specified weight. This is considered to be a difficult problem to solve in general, but certain special cases of the problem are relatively easy to solve, which serve as the "trapdoor" of the system. The-single iteration knapsack cryptosystem introduced in 1978 was broken by Shamir. Merkle then published the multiple-iteration knapsack problem which was broken by Brickell [Bri85]. Merkle offered a $100 reward for anybody able to crack the single iteration knapsack and a $1000 reward for anybody able to crack the multiple iteration cipher from his own pocket. When they were cracked, he promptly paid up.

**Read More Answers.**

# Cryptography Most Popular Interview Topics.

1 : Cryptography General Frequently Asked Interview Questions and Answers Guide.

2 : Cryptography Frequently Asked Interview Questions and Answers Guide.

3 : Digital Certificates Frequently Asked Interview Questions and Answers Guide.

4 : Ciphers Frequently Asked Interview Questions and Answers Guide.

5 : Cryptography Algorithm Frequently Asked Interview Questions and Answers Guide.

6 : Typist Frequently Asked Interview Questions and Answers Guide.

7 : Cryptography Protocols Frequently Asked Interview Questions and Answers Guide.

8 : Typesetter Frequently Asked Interview Questions and Answers Guide.

9 : Cryptography Teacher Frequently Asked Interview Questions and Answers Guide.

# About Global Guideline.

**Global Guideline** is a platform to develop your own skills with thousands of job interview questions and web tutorials for fresher's and experienced candidates. These interview questions and web tutorials will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts. Global Guideline invite you to unlock your potentials with thousands of **Interview Questions with Answers** and much more. Learn the most common technologies at Global Guideline. We will help you to explore the resources of the World Wide Web and develop your own skills from the basics to the advanced. Here you will learn anything quite easily and you will really enjoy while learning. Global Guideline will help you to become a professional and Expert, well prepared for the future.

* This PDF was generated from https://GlobalGuideline.com at **November 29th, 2023**

* If any answer or question is incorrect or inappropriate or you have correct answer or you found any problem in this document then don't hesitate feel free and e-mail us we will fix it.

You can follow us on FaceBook for latest Jobs, Updates and other interviews material.
www.facebook.com/InterviewQuestionsAnswers

Follow us on Twitter for latest Jobs and interview preparation guides
https://twitter.com/InterviewGuide

Best Of Luck.

Global Guideline Team
https://GlobalGuideline.com
Info@globalguideline.com