Cryptography Teacher Interview Questions And Answers Guide.

Global Guideline.

https://globalguideline.com/

Cryptography Teacher Job Interview Preparation Guide.

Question # 1

Tell me what is Cryptography?

Answer:-

Cryptography is the art and science of making a cryptosystem that is capable of providing information security.
Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

Read More Answers.

Question # 2

Explain me types of Cryptosystems?

Answer:-

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system -
Symmetric Key Encryption
Asymmetric Key Encryption
The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Read More Answers.

Question # 3

Explain me Monoalphabetic and Polyalphabetic Cipher?

Answer:-

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.
All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalysis.
Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, playfair and Vigenere Cipher are polyalphabetic ciphers.

Read More Answers.

Question # 4

What is RSA Cryptosystem?

Answer:-

This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem.
We will see two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms.

Read More Answers.

Question # 5

What is Elliptic Curve Cryptography (ECC)?

Answer:-

Elliptic Curve Cryptography (ECC) is a term used to describe a suite of cryptographic tools and protocols whose security is based on special versions of the discrete logarithm problem. It does not use numbers modulo p.
ECC is based on sets of numbers that are associated with mathematical objects called elliptic curves. There are rules for adding and computing multiples of these numbers, just as there are for numbers modulo p.
ECC includes a variants of many cryptographic schemes that were initially designed for modular numbers such as ElGamal encryption and Digital Signature Algorithm.
It is believed that the discrete logarithm problem is much harder when applied to points on an elliptic curve. This prompts switching from numbers modulo p to points on an elliptic curve. Also an equivalent security level can be obtained with shorter keys if we use elliptic curve-based variants.
The shorter keys result in two benefits -
Ease of key management

Efficient computation

Read More Answers.

Question # 6

On perform the Mix Columns transformation for the sequence of bytes "77 89 AB CD" we get output
a) {01 55 EE 4A}
b) {0A 44 EF 4A}
c) {08 55 FF 3A}
d) {09 44 DD 4A}

Answer:-

c) {08 55 FF 3A}
Explanation: Perform the mix columns transformation to obtain the output {08 55 FF 3A}.

Read More Answers.

Question # 7

S-AES and S-DES were both developed by the same person as an educational cryptography system to teach students
a) True
b) False

Answer:-

a) True

Read More Answers.

Question # 8

A substitution cipher substitutes one symbol with
Keys
Others
Multi Parties
Single Party

Answer:-

Others

Read More Answers.

Question # 9

In cryptography, the order of the letters in a message is rearranged by:
A. transpositional ciphers B. substitution ciphers C. both (a) and (b) D. none of the mentioned

Answer:-

A. transpositional ciphers

Read More Answers.

Question # 10

We use Cryptography term to transforming messages to make them secure and immune to
Change
Idle
Attacks
Defend

Answer:-

Attacks

Read More Answers.

Question # 11

Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not
Authenticated
Joined
Submit
Separate

Answer:-

Authenticated

Read More Answers.

Question # 12

Cryptographic hash function takes an arbitrary block of data and returns:
A. fixed size bit string B. variable size bit string C. both (a) and (b) D. none of the mentioned

Answer:-

A. fixed size bit string

Read More Answers.

Question # 13

Which one of the following is a cryptographic protocol used to secure HTTP connection?
A. stream control transmission protocol (SCTP) B. transport layer security (TSL) C. explicit congestion notification (ECN) D. resource reservation protocol

Answer:-

B. transport layer security (TSL)

Read More Answers.

Question # 14

1. How many computation rounds does the simplified AES consists of?
a) 5
b) 2
c) 8
d) 10

Answer:-

a) 5
Explanation: The simplified AES has only 2 rounds of computation.

Read More Answers.

Question # 15

An asymmetric-key (or public-key) cipher uses
1 Key
2 Key
3 Key
4 Key

Answer:-

2 Key

Read More Answers.

Question # 16

ElGamal encryption system is:
A. symmetric key encryption algorithm B. asymmetric key encryption algorithm C. not an encryption algorithm D. none of the mentioned

Answer:-

B. asymmetric key encryption algorithm

Read More Answers.

Question # 17

On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?
a) f function
b) permutation p
c) swapping of halves
d) xor of subkey with function f

Answer:-

c) swapping of halves
Explanation: There is no equivalent to swapping of halves in the AES algorithm.

Read More Answers.

Question # 18

Cryptanalysis is used:
A. to find some insecurity in a cryptographic scheme B. to increase the speed C. to encrypt the data D. none of the mentioned

Answer:-

A. to find some insecurity in a cryptographic scheme

Read More Answers.

Question # 19

For the case of Mixed Columns and Inverse Mixed Columns, is it true that b(x) = a-1(x)mod(x4 + 1)
where a(x) = {03}x3 + {01}x2 + {01}x + {02} and b(x) = {0B}x3 + {0D}x2 + {09}x + {0E}
a) True
b) False. The expression for a(x) is wrong.
c) False. The expression for b(x) is wrong.
d) False. Both a(x) and b(x) are faulty.

Answer:-

a) True
Explanation: The statment is true and can be checked as it is similar to the matrix forms of mixed columns and inverse mixed columns.

Read More Answers.

Question # 20

On perform the Mix Columns transformation for the sequence of bytes "67 89 AB CD" we get output
a) {08 55 FF 18}
b) {28 45 EF 08}
c) {28 45 FF 18}
d) {25 35 EF 08}

Answer:-

b) {28 45 EF 08}
Explanation: Perform the mix columns transformation to obtain the output {28 45 EF 0A}.

Read More Answers.

Question # 21

What is the block size in the Simplified AES algorithm?
a) 8 bits
b) 40 bits
c) 16 bits
d) 36 bits

Answer:-

b) 40 bits
Explanation: The block size for the AES algorithm is 16 bits.

Read More Answers.

Question # 22

A straight permutation cipher or a straight P-box has same number of inputs as
cipher
Frames
Outputs
Bits

Answer:-

Outputs

Read More Answers.

Question # 23

Voice privacy in GSM cellular telephone protocol is provided by:
A. A5/2 cipher B. b5/4 cipher C. b5/6 cipher D. b5/8 cipher

Answer:-

A. A5/2 cipher

Read More Answers.

Question # 24

In cryptography, what is cipher?
A. algorithm for performing encryption and decryption B. encrypted message C. both (a) and (b) D. none of the mentioned

Answer:-

A. algorithm for performing encryption and decryption

Read More Answers.

Question # 25

Which of the following is a faulty S-AES step function?
a) Add round key
b) Byte substitution
c) Shift rows
d) Mix Columns

Answer:-

b) Byte substitution
Explanation: The correct version in S-AES would be nibble substitution as 4 bits are taken at a time.

Read More Answers.

Question # 26

Is the following matrix the inverse matrix of the matrix used in the mix columns step?
x3 + 1 x
x x3 + 1
a) Yes
b) No
c) Can't say
d) Insufficient Information

Answer:-

a) Yes
Explanation: On multiplying this matrix with the mix columns matrix we get the identity matrix, this proves that it is an inverse matrix.

Read More Answers.

Question # 27

For an inputs key of size 128 bits constituting of all zeros, what is w(7) ?
a) {62 63 63 63}
b) {62 62 62 62}
c) {00 00 00 00}
d) {63 63 63 62}

Answer:-

a) {62 63 63 63}
Explanation: Applying the key algorithm we get,
w(0) = {00 00 00 00}; w(1) = {00 00 00 00}; w(2) = {00 00 00 00}; w(3) = {00 00 00 00};
w(4) = {62 63 63 63}; w(5) = {62 63 63 63}; w(6) = {62 63 63 63}; w(7) = {62 63 63 63}

Read More Answers.

Question # 28

In asymmetric key cryptography, the private key is kept by:
A. sender B. receiver C. sender and receiver D. all the connected devices to the network

Answer:-

B. receiver

Read More Answers.

Question # 29

What is data encryption standard (DES)?
A. block cipher B. stream cipher C. bit cipher D. none of the mentioned

Answer:-

A. block cipher

Read More Answers.

Question # 30

For the cipher text 0000 0111 0011 1000 and Key 0110 1111 0110 1011, apply the Simplified AES to obtain the plaintext. The plain text is
a) 0110 1001 0111 0001
b) 0110 1111 0110 1011
c) 0010 1001 0110 1011
d) 1111 0101 0111 1111

Answer:-

b) 0110 1111 0110 1011
Explanation: On applying the simplified AES we would obtain 0110 1111 0110 1011 as the plain text.

Read More Answers.

Question # 31

Which one of the following algorithm is not used in asymmetric-key cryptography?
A. RSA algorithm B. diffie-hellman algorithm C. electronic code book algorithm D. none of the mentioned

Answer:-

C. electronic code book algorithm

Read More Answers.

Question # 32

What is the key size in the S-AES algorithm?
a) 16 bits
b) 32 bits
c) 24 bits
d) None of the mentioned

Answer:-

a) 16 bits
Explanation: The key size in the S-AES algorithm is 16 bits.

Read More Answers.

Question # 33

Explain components of a Cryptosystem?

Answer:-

The various components of a basic cryptosystem are as follows -
Plaintext. It is the data to be protected during transmission.
Encryption Algorithm. It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
Ciphertext. It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It

flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
Decryption Algorithm, It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
Encryption Key. It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
Decryption Key. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

Read More Answers.

Question # 34

Explain Kerckhoff's Principle for Cryptosystem?

Answer:-

In the 19th century, a Dutch cryptographer A. Kerckhoff furnished the requirements of a good cryptosystem. Kerckhoff stated that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge. The six design principles defined by Kerckhoff for cryptosystem are -
The cryptosystem should be unbreakable practically, if not mathematically.
Falling of the cryptosystem in the hands of an intruder should not lead to any compromise of the system, preventing any inconvenience to the user.
The key should be easily communicable, memorable, and changeable.
The ciphertext should be transmissible by telegraph, an unsecure channel.
The encryption apparatus and documents should be portable and operable by a single person.
Finally, it is necessary that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Read More Answers.

Question # 35

Tell me what can you use to defend against multiple login attempts?

Answer:-

You can create a lockout policy that locks accounts when a user has too many login attempts.

Read More Answers.

Question # 36

Explain me what is Diffie-Hellman?

Answer:-

It is a method by which a key can be securely shared by two users without any actual exchange.

Read More Answers.

Question # 37

Tell me what are MD2, MD4, and MD5?

Answer:-

MD2, MD4 and MD5 are 128 bit hashing algorithms

Read More Answers.

Question # 38

Explain me what is Cryptanalysis?

Answer:-

The art and science of breaking the cipher text is known as cryptanalysis.
Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.
Note - Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

Read More Answers.

Question # 39

Do you know advanced Encryption Standard?

Answer:-

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.
The features of AES are as follows -
* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

Read More Answers.

Question # 40

Tell me what is the difference between a public key cryptography and a private key for encrypting and signing content?

Answer:-

A send or recipient publishes his public key. You use the public key to encrypt content and your private key to sign the content. This is the standard form of communication with encryption and signing.

Read More Answers.

Question # 41

Tell me how can you defend against phishing attempts?

Answer:-

Phishing is usually done through email, so you can block some SMTP servers, senders, and educate users on phishing attempts.

Read More Answers.

Question # 42

Tell me how would an HTTP program handle state?

Answer:-

HTTP does not handle state natively. HTTP applications use cookies to handle the state of an application. The developer can also store data in the web server's session.

Read More Answers.

Question # 43

Explain me what is RC4?

Answer:-

RC4 is a symmentric key, cryptographic algorithm developed by Ron Rivest. It uses stream cipher to create variable size keys.

Read More Answers.

Question # 44

What is ElGamal Cryptosystem?

Answer:-

Along with RSA, there are other public-key cryptosystems proposed. Many of them are based on different versions of the Discrete Logarithm Problem.
ElGamal cryptosystem, called Elliptic Curve Variant, is based on the Discrete Logarithm Problem. It derives the strength from the assumption that the discrete logarithms cannot be found in practical time frame for a given number, while the inverse operation of the power can be computed efficiently.
Let us go through a simple version of ElGamal that works with numbers modulo p. In the case of elliptic curve variants, it is based on quite different number systems.

Read More Answers.

Question # 45

Explain me what should be implemented on a login page?

Answer:-

Whenever you transfer sensitive data, you need to use HTTPS. Ensure you answer this question with HTTPS and possibly how you would implement a conversion of HTTP to HTTPS.

Read More Answers.

Question # 46

Explain what is RC5?

Answer:-

RC5 is the coding technique through which IR remote button keycode are coded and transmitted to the receiver......

Read More Answers.

Question # 47

Tell me what are some ways that the company can defend against XSS?

Answer:-

First, the programmers should defend against JS script added to a querystring. Also, remove JS from any input variables send through online forms and stored in a database.

Read More Answers.

Question # 48

Explain me RSA Analysis?

Answer:-

The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.
Encryption Function - It is considered as a one-way function of converting plaintext into ciphertext and it can be reversed only with the knowledge of private key d.
Key Generation - The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p & q values to modulus n is easy but reverse is not possible.

Read More Answers.

Question # 49

What is symmetric Key Encryption?

Answer:-

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.
The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.

Read More Answers.

Question # 50

Do you know what is Cross Site Scripting or XSS?

Answer:-

Cross site scripting occurs when an attacker is able to inject executable code within JavaScript. This is done through a hacked database or poorly scrubbed querystring variables.

Read More Answers.

Question # 51

Explain me what are the two types of XSS?

Answer:-

Cross site scripting has two types of attacks: reflected and stored. A stored XSS hack allows the attacker to store malicious code within the database. The database content is served to the user from the database and can be used in private pages behind a secure login to gain access to site private data. The next is reflected, and this comes from the hacker sending the user a link that runs JS code within the pages directly from the querystring.

Read More Answers.

Question # 52

Explain me about your home network?

Answer:-

Although there is no right answer for this question, it helps the candidate relax, while pushing them off script. From there, try probing into details and ask relevant questions about decisions.
Understanding how a person thinks about cybersecurity is just as important as knowing about the controls. Following the discussion as to why the candidate made specific decisions, you are likely to be asked, "What is the goal of information security within an organization?"
This helps the interviewer understand what you think about the role. Are you authoritarian and will be ready to stop the project because of a risk or is there a better way? This will also help them answer if the applicant is trustworthy.

Read More Answers.

Question # 53

Tell me do you prefer Windows or Linux?

Answer:-

This question is more of a preference, but many network security professionals know linux to work with security. For instance, Linux is better to know when working with routers. Be honest with your answer and give pros and cons that relate to which one you prefer.

Read More Answers.

Question # 54

Explain me what port is for ICMP or pinging?

Answer:-

Ping uses the ICMP protocol, which is a layer 3 protocol. Ping doesn't use a port, so you want to note that this is a trick question if asked.

Read More Answers.

Question # 55

What is asymmetric Key Encryption?

Answer:-

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible.

Read More Answers.

Cryptography Most Popular Interview Topics.

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

2 : Encryption Decryption Frequently Asked Interview Questions and Answers Guide.

3 : Cryptography Frequently Asked Interview Questions and Answers Guide.

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

5 : Ciphers Frequently Asked Interview Questions and Answers Guide.

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

7 : Typist Frequently Asked Interview Questions and Answers Guide.

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

9 : Typesetter 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