Cryptography Teacher Job Interview Questions And Answers

Interview Questions Answers

https://interviewquestionsanswers.org/

About Interview Questions Answers

Interview Questions Answers . ORG is an interview preparation guide of thousands of Job Interview Questions And Answers, Job Interviews are always stressful even for job seekers who have gone on countless interviews. The best way to reduce the stress is to be prepared for your job interview. Take the time to review the standard interview questions you will most likely be asked. These interview questions and answers on Cryptography Teacher will help you strengthen your technical skills, prepare for the interviews and quickly revise the concepts.

If you find any **question or answer** is incorrect or incomplete then you can **submit your question or answer** directly with out any registration or login at our website. You just need to visit Cryptography Teacher Interview Questions And Answers to add your answer click on the *Submit Your Answer* links on the website; with each question to post your answer, if you want to ask any question then you will have a link *Submit Your Question*; that's will add your question in Cryptography Teacher category. To ensure quality, each submission is checked by our team, before it becomes live. This Cryptography Teacher Interview preparation PDF was generated at **Wednesday 29th November, 2023**

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

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

If you need any further assistance or have queries regarding this document or its material or any of other inquiry, please do not hesitate to contact us.

Best Of Luck.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
Support@InterviewQuestionsAnswers.ORG

Cryptography Teacher Interview Questions And Answers Guide.

Question - 1:

What is asymmetric Key Encryption?

Ans:

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.

View All Answers

Question - 2:

Explain me what port is for ICMP or pinging?

Ans:

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.

View All Answers

Question - 3:

Tell me do you prefer Windows or Linux?

Ans:

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.

View All Answers

Question - 4:

Explain me about your home network?

Ans:

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.

View All Answers

Question - 5:

Explain me what are the two types of XSS?

Ans:

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.

View All Answers

Question - 6:

Do you know what is Cross Site Scripting or XSS?

Ans:

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.

View All Answers

Question - 7:

What is symmetric Key Encryption?

Ans:

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.

View All Answers

Question - 8:

Explain me RSA Analysis?

Ans:

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.

View All Answers

Question - 9:

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

Ans:

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.

View All Answers

Question - 10:

Explain what is RC5?

Ans:

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

View All Answers

Question - 11:

Explain me what should be implemented on a login page?

Ans:

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.

View All Answers

Question - 12:

What is ElGamal Cryptosystem?

Ans:

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.

View All Answers

Question - 13:

Explain me what is RC4?

Ans:

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

View All Answers

Question - 14:

Tell me how would an HTTP program handle state?

Ans:

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.

View All Answers

Question - 15:

Tell me how can you defend against phishing attempts?

Ans:

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

View All Answers

Question - 16:

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

Ans:

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.

View All Answers

Question - 17:

Do you know advanced Encryption Standard?

Ans:

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

View All Answers

Question - 18:

Explain me what is Cryptanalysis?

Ans:

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.

View All Answers

Question - 19:

Tell me what are MD2, MD4, and MD5?

Ans:

MD2, MD4 and MD5 are 128 bit hashing algorithms

View All Answers

Question - 20:

Explain me what is Diffie-Hellman?

Ans:

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

View All Answers

Question - 21:

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

Ans:

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

View All Answers

Question - 22:

Explain Kerckhoff's Principle for Cryptosystem?

Ans:

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.

View All Answers

Question - 23:

Explain components of a Cryptosystem?

Ans:

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.

View All Answers

Question - 24:

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

Ans:

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

View All Answers

Question - 25:

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

Ans:

C. electronic code book algorithm

View All Answers

Question - 26:

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

Ans:

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

View All Answers

Question - 27:

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

Ans:

A. block cipher

View All 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

Ans:

B. receiver

View All Answers

Question - 29:

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}

Ans:

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}

View All Answers

Question - 30:

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

Ans:

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.

View All Answers

Question - 31:

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

Ans:

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

View All Answers

Question - 32:

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

Ans:

A. algorithm for performing encryption and decryption

View All Answers

Question - 33:

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

Ans:

A. A5/2 cipher

View All Answers

Question - 34:

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

Ans:

Outputs

View All Answers

Question - 35:

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

Ans:

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

View All Answers

Question - 36:

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}

Ans:

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

View All Answers

Question - 37:

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.

Ans:

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.

View All Answers

Question - 38:

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

Ans:

A. to find some insecurity in a cryptographic scheme

View All Answers

Question - 39:

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

Ans:

Others

View All Answers

Question - 40:

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

Ans:

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

View All Answers

Question - 41:

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

Ans:

B. asymmetric key encryption algorithm

View All Answers

Question - 42:

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

Ans:

2 Key

View All Answers

Question - 43:

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

Ans:

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

View All Answers

Question - 44:

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

Ans:

B. transport layer security (TSL)

View All Answers

Question - 45:

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

Ans:

A. fixed size bit string

View All Answers

Question - 46:

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

Ans:

Authenticated

View All Answers

Question - 47:

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

Ans:

Attacks

View All Answers

Question - 48:

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

Ans:

A. transpositional ciphers

View All Answers

Question - 49:

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

Ans:

a) True

View All Answers

Question - 50:

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}

Ans:

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

View All Answers

Question - 51:

What is Elliptic Curve Cryptography (ECC)?

Ans:

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

View All Answers

Question - 52:

What is RSA Cryptosystem?

Ans:

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.

View All Answers

Question - 53:

Explain me Monoalphabetic and Polyalphabetic Cipher?

Ans:

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.

View All Answers

Question - 54:

Explain me types of Cryptosystems?

Ans:

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.

View All Answers

Question - 55:

Tell me what is Cryptography?

Ans:

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.

View All Answers

Cryptography Most Popular & Related Interview Guides

1 : **Cryptography General Interview Questions and Answers.**

2 : Typesetter Interview Questions and Answers.

3 : Ciphers Interview Questions and Answers.

4 : Typewriter Interview Questions and Answers.

5 : Cryptography Interview Questions and Answers.

6 : Encryption Decryption Interview Questions and Answers.

7 : Digital Certificates Interview Questions and Answers.

8 : Cryptography Algorithm Interview Questions and Answers.

9 : Cryptography Protocols Interview Questions and Answers.

Follow us on FaceBook
www.facebook.com/InterviewQuestionsAnswers.Org

Follow us on Twitter
https://twitter.com/InterviewQA

For any inquiry please do not hesitate to contact us.

Interview Questions Answers.ORG Team
https://InterviewQuestionsAnswers.ORG/
support@InterviewQuestionsAnswers.ORG