Cryptography Protocols Interview Questions And Answers Guide.

Global Guideline.

https://globalguideline.com/

Cryptography Protocols Job Interview Preparation Guide.

Question # 1

What is PEM?

Answer:-

PEM is the draft Internet Privacy-Enhanced Mail standard, designed, proposed, but not yet officially adopted, by the Internet Activities Board to provide secure electronic mail over the Internet. Designed to work with RFC 822 e-mail formats, PEM includes encryption, authentication, and key management, and allows use of both public-key and secret-key cryptosystems. Multiple cryptographic tools are supported; for each mail message, the specific encryption algorithm, digital signature algorithm, hash function, and so on are specified in the header. PEM explicitly supports only a few cryptographic algorithms; others may be added later. DES in CBC mode is currently the only message encryption algorithm supported, and both RSA and DES are supported for key management. Public-key management in PEM is based on X.509 certificates.

Read More Answers.

Question # 2

What is SSL (Secure Socket Layer)?

Answer:-

The SSL (Secure Socket Layer) Handshake Protocol was developed by Netscape Communications Corporation to provide security and privacy over the Internet. The protocol supports server and client authentication. The SSL protocol is application independent, allowing protocols like HTTP, FTP (File Transfer Protocol), and Telnet to be layered on top of it transparently. The SSL protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by the higher-level application. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

Read More Answers.

Question # 3

What is the Difference Between SSL and S-HTTP?

Answer:-

The main difference between the protocols is the layer at which they operate. SSL operates at the transport layer and mimics the "socket library," while S-HTTP operates at the application layer. Encryption of the transport layer allows SSL to be application-independent, while S-HTTP is limited to the specific software implementing it. The protocols adopt different philosophies towards encryption as well, with SSL encrypting the entire communications channel and S-HTTP encrypting each message independently. S-HTTP allows a user to produce digital signatures on any messages (not just specific messages during an authentication protocol), a feature SSL lacks. Terisa Systems is developing toolkits to support both protocols.

Read More Answers.

Question # 4

What is S/MIME?

Answer:-

S/MIME (Secure/ Multipurpose Internet Mail Extensions) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages described in RFC 1521. MIME is the official proposed standard format for extended Internet electronic mail. Internet e-mail messages consist of two parts, the header and the body. The header forms a collection of field/value pairs structured to provide information essential for the transmission of the message. The structure of the headers can be found in RFC 822. The body is normally unstructured unless the e-mail is in MIME format. MIME defines how the body of an e-mail message is structured. The MIME format permits e-mail to include enhanced text, graphics, audio, and more in a standardized manner via MIME-compliant mail systems. However, MIME itself does not provide any security services. The purpose of S/MIME is to define such services, following the syntax given in PKCS #7 for digital signatures and encryption. The MIME body part carries a PKCS #7 message, which itself is the result of cryptographic processing on other MIME body parts.

Read More Answers.

Question # 5

What is PEM-MIME, or What is MOSS?

Answer:-

PEM-MIME, also known as MIME Object Security Standard or MOSS, is a proposed Internet Draft [CFG95] that is designed to be a successor to PEM. It proposes adding PEM- based security services to MIME messages in much the same manner as S/MIME. Due to the nature of MIME, it is possible to apply different security

services to each part of the body. For example, the MIME body may contain two copies of a message, with one copy digitally signed and the other copy not modified in any way. This will allow a recipient to read the message even if the recipient does not have a MIME-compliant mail reader. If the recipient has a privacy-enhanced MIME compliant mail reader, the recipient will be able to verify the digital signature as well. Another possibility would be to encrypt different blocks of the message body using different keys and algorithms, or to sign some blocks and not others need not b.

Read More Answers.

Question # 6

What is S-HTTP?

Answer:-

S-HTTP (Secure Hypertext Transfer Protocol) is an extension to HTTP (Hypertext Transfer Protocol) that provides security services. It was originally developed by Enterprise Integration Technologies, and further development continues at Terisa Systems. HTTP is the protocol that forms the basis of the World Wide Web, allowing the exchange of multimedia documents on the Web. S-HTTP is designed to provide confidentiality, authenticity, integrity, and non-repudiability while supporting multiple key management mechanisms and cryptographic algorithms via option negotiation between the parties involved in each transaction.

Read More Answers.

Question # 7

What is PCT?

Answer:-

PCT stands for Private Communication Technology, a protocol developed by Microsoft and Visa International for secure communication on the Internet. It is a counterpart to Netscape's SSL protocol and a companion to the STT protocol. Like SSL, PCT is intended for Internet standardization.
The protocol is quite similar to SSL in many respects, and in fact the message formats are similar enough so that a server can interact with clients supporting SSL as well as client supporting PCT. According to the specification, PCT "corrects or improves on several weaknesses of SSL." The following are the main differences:
PCT involves fewer messages between the client and the server than SSL, and the messages themselves are shorter.
PCT has more choices in the negotiation of algorithm and data formats than SSL, and the negotiation has additional cryptographic protection so that the client and server can verify that their choices have not been modified.

Read More Answers.

Question # 8

What is S/WAN?

Answer:-

The S/WAN (Secure Wide Area Network, pronounced "swan") initiative designates specifications for implementing IPSec, the security architecture for the Internet Protocol, to ensure interoperability among firewall and TCP/IP products. S/WAN's goal is to use IPSec to allow companies to mix-and-match the best firewall and TCP/IP stack products to build Internet-based Virtual Private Networks (VPNs). Currently, users and administrators are often locked in to single-vendor solutions network-wide, because vendors have been unable to agree upon the details of IPSec implementation. The S/WAN effort should therefore remove a major obstacle to the widespread deployment of secure VPNs.

Read More Answers.

Question # 9

Given that messages belong to the set {0,1,2},create shamirs authentication scheme with randomization?

Answer:-

select p,q
compute n=p*q

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 : 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