Network Security

Multiple Choice Question & Answer:-

MCQ. Confidentiality with asymmetric-key cryptosystem has its own

A.System.

B.Data.

C.Problems.

D.Issues.

Answer C

MCQ. SHA-l has a message digest of

A.160 bits.

B.512 bits.

C.628 bits.

D.820 bits.

Answer A

MCQ. Message authentication is a service beyond

A.Message Confidentiality.

B.Message Integrity.

C.Message Splashing.

D.Message Sending.

Answer B

MCQ. In Message Confidentiality, transmitted message must make sense to only intended

A.Receiver.

B.Sender.

C.Third Party.

D.Translator.

Answer A

MCQ. A hash function guarantees integrity of a message. It guarantees that message has not be

A.Replaced.

B.Over view.

C.Changed.

D.Left.

Answer C

MCQ. To check integrity of a message, or document, receiver creates the

A.Tag.

B.Hash Tag.

C.Hyper Text.

D.Finger Print.

Answer B

MCQ. A digital signature needs a

A.private-key system.

B.shared-key system.

C.public-key system.

D.All of them.

Answer C

MCQ. One way to preserve integrity of a document is through use of a

A.Thumb Impression.

B.Finger Print.

C.Biometric.

D.X-Rays.

Answer B

MCQ. A session symmetric key between two parties is used

A.only once.

B.twice.

C.multiple times.

D.depends on situation.

Answer A

MCQ. Encryption and decryption provide secrecy, or confidentiality, but not

A.Authentication.

B.Integrity.

C.Keys.

D.Frames.

Answer B

MCQ. MAC stands for

A.message authentication code.

B.message authentication connection.

C.message authentication control.

D.message authentication cipher.

Answer A

MCQ. Digest created by a hash function is normally called a

A.modification detection code (MDC).

B.message authentication connection.

C.message authentication control.

D.message authentication cipher.

Answer A

MCQ. Message confidentiality is using

A.Cipher Text.

B.Cipher.

C.Symmetric-Key.

D.Asymmetric-Key.

Answer D

MCQ. A sender must not be able to deny sending a message that he or she, in fact, did send, is known as

A.Message Nonrepudiation.

B.Message Integrity.

C.Message Confidentiality.

D.Message Sending.

Answer A

MCQ. To preserve integrity of a document, both document and fingerprint are

A.Important.

B.System.

C.Needed.

D.Not needed.

Answer C

MCQ. When data must arrive at receiver exactly as they were sent, its called

A.Message Confidentiality.

B.Message Integrity.

C.Message Splashing.

D.Message Sending.

Answer B

MCQ. Message digest needs to be

A.public.

B.private.

C.kept secret.

D.None.

Answer C

MCQ. In Message Integrity, message digest needs to be kept

A.Secret.

B.Low.

C.High.

D.Down.

Answer A

MCQ. In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of

A.512 Bit Blocks.

B.1001 Bit Blocks.

C.1510 Bit Blocks.

D.2020 Bit Blocks.

Answer A

MCQ. Message confidentiality or privacy means that sender and receiver expect

A.Integrity.

B.Confidentiality.

C.Authentication.

D.Nonrepudiation.

Answer B

MCQ. Message must be encrypted at sender site and decrypted at the

A.Sender Site.

B.Site.

C.Receiver site.

D.Conferencing.

Answer C

MCQ. Encrypted security payload extension header is new in

A.Ipv4.

B.IPv5.

C.IPv6.

D.None.

Answer C

MCQ. Performance, reliability, and security are criteria of

A.Efficient network.

B.intranet.

C.protocols.

D.None of Above.

Answer A

MCQ. Data Encryption Standard (DES) was designed by

A.Microsoft.

B.Apple.

C.IBM.

D.None.

Answer C

MCQ. One of protocols to provide security at application layer is

A.Pretty Good Privacy.

B.Handshake Protocol.

C.Alert Protocol.

D.Record Protocol.

Answer A