QUESTION 725
Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

A. Diffie-Hellman Key Exchange Protocol
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY

Correct Answer: D

QUESTION 726
Which of the following defines the key exchange for Internet Protocol Security (IPSEC)?

A. Internet Security Association Key Management Protocol (ISAKMP)
B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Communication Messaging Protocol (ICMP)

Correct Answer: A

QUESTION 727
A network of five nodes is using symmetrical keys to securely transmit data. How many new keys are required to re-establish secure communications to all nodes in the event there is a key compromise?

A. 5
B. 10
C. 20
D. 25

Correct Answer: B

QUESTION 728
What is the effective key size of DES?

A. 56 bits
B. 64 bits
C. 128 bits
D. 1024 bits

Correct Answer: A

QUESTION 729
Matches between which of the following are important because they represent references from one relation to another and establish the connection among these relations?

A. foreign key to primary key
B. foreign key to candidate key
C. candidate key to primary key
D. primary key to secondary key

Correct Answer: A

QUESTION 730
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets?

A. Internet Security Association and Key Management Protocol (ISKAMP)
B. Simple Key-Management for Internet Protocols (SKIP)
C. Diffie-Hellman Key Distribution Protocol
D. IPsec Key Exchange (IKE)

Correct Answer: B

QUESTION 731
What is the PRIMARY advantage of secret key encryption systems as compared with public key systems?

A. Faster speed encryption
B. Longer key lengths
C. Easier key management
D. Can be implemented in software

Correct Answer: A

QUESTION 732
In a cryptographic key distribution system, the master key is used to exchange?

A. Session keys
B. Public keys

C. Secret keys
D. Private keys

Correct Answer: A

QUESTION 733
Which Application Layer security protocol requires two pair of asymmetric keys and two digital certificates?

A. PEM
B. S/HTTP
C. SET
D. SSL

Correct Answer: C

QUESTION 734
Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?

A. foreign key
B. candidate key
C. Primary key
D. Secondary key

Correct Answer: A

QUESTION 735
What key size is used by the Clipper Chip?

A. 40 bits
B. 56 bits
C. 64 bits
D. 80 bits

Correct Answer: D

QUESTION 736
What uses a key of the same length as the message?

A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining

Correct Answer: B

QUESTION 737
Which of the following statements related to a private key cryptosystem is FALSE?

A. The encryption key should be secure.
B. Data Encryption Standard (DES) is a typical private key cryptosystem.
C. The key used for decryption is known to the sender.
D. Two different keys are used for the encryption and decryption.

Correct Answer: D

QUESTION 738
Simple Key Management for Internet Protocols (SKIP) is similar to Secure Sockets Layer (SSL), except that it requires no prior communication in order to establish or exchange keys on a:

A. Secure Private keyring basis
B. response-by-session basis
C. Remote Server basis
D. session-by-session basis

Correct Answer: D

QUESTION 739
A weak key of an encryption algorithm has which of the following properties?

A. It is too short, and thus easily crackable.
B. It facilitates attacks against the algorithm.
C. It has much more zeroes than ones.
D. It can only be used as a public key.

Correct Answer: B

QUESTION 740
Security measures that protect message traffic independently on each communication path are called:

A. Link oriented
B. Procedure oriented
C. Pass-through oriented
D. End-to-end oriented

Correct Answer: A

QUESTION 741
Who is responsible for the security and privacy of data during a transmission on a public communications link?

A. The carrier.
B. The sending party.
C. The receiving party.
D. The local service provider.

Correct Answer: B

QUESTION 742
Which of the following best provides e-mail message authenticity and confidentiality?

A. Signing the message using the sender's public key and encrypting the message using the receiver's private key.
B. Signing the message using the sender's private key and encrypting the message using the receiver's public key.
C. Signing the message using the receiver's private key and encrypting the message using the sender's public key.
D. Signing the message using the receiver's public key and encrypting the message with the sender's private key.

Correct Answer: B

QUESTION 743
Cryptography does not help in:

A. Detecting fraudulent insertion
B. Detecting fraudulent deletion