QUESTION 802
What enables users to validate each other's certificate when they are certified under different certification hierarchies?

A. Cross-certification
B. Multiple certificates
C. Redundant certificate authorities
D. Root certification authorities

Correct Answer: A

QUESTION 803
Digital signature users register their public keys with a certification authority, which distributes a certificate containing the user's public key and digital signature of the certification authority. In creating the certificate, the user's public key and the validity period are combined with what other information before computing the digital signature?

A. Certificate issuer and the Digital Signature Algorithm identifier.
B. User's private key and the identifier of the master key code.
C. Name of secure channel and the identifier of the protocol type.
D. Key authorization and identifier of key distribution center.

Correct Answer: A

QUESTION 804
What level of assurance for digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

A. Level 1
B. Level 2
C. Level 3
D. Level 4

Correct Answer: B

QUESTION 805
Which one of the following security technologies provides safeguards for authentication before securely sending information to a web server?

A. Secure/Multipurpose Internet Mail Extension (S/MIME)
B. Common Gateway Interface (CGI) scripts

C. Applets

D. Certificates

Correct Answer: D

QUESTION 806

The primary role of cross certification is:

A. Creating trust between different PKIs.

B. Build an overall PKI hierarchy.

C. Set up direct trust to a second root CA.

D. Prevent the nullification of user certifications by CA certificate revocation.

Correct Answer: A

QUESTION 807

Windows 98 includes the ability to check the digitally signed hardware drivers. Which of the following are true?

A. Drivers are the only files supplied with W98 that can checked for digital signatures and all drivers included with W98 have been digitally signed.

B. If a file on a windows W98 has been digitally signed it means that the file has passed quality testing by Microsoft.

C. The level to which signature checking is implemented could only be changed by editing the registry.

D. All of the statements are true

Correct Answer: B

QUESTION 808

What is the purpose of certification path validation?

A. Checks the legitimacy of the certificates in the certification path.

B. Checks that all certificates in the certification path refer to same certification practice statement.

C. Checks that no revoked certificates exist outside the certification path.

D. Checks that the names in the certification path are the same.

Correct Answer: A

QUESTION 809
In what type of attack does an attacker try, from several encrypted messages, to figure out the key using the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Known Ciphertext attack

Correct Answer: B

QUESTION 810
When combined with unique session values, message authentication can protect against which of the following?

A. Reverse engineering, frequency analysis, factoring attacks, and ciphertext-only attack.
B. Masquerading, frequency analysis, sequence manipulation, and ciphertext-only attack.
C. Reverse engineering, content modification, factoring attacks, and submission notification.
D. Masquerading, content modification, sequence manipulation, and submission notification.

Correct Answer: C

QUESTION 811
The relative security of a commercial cryptographic system can be measured by the?

A. Rating value assigned by the government agencies that use the system.
B. Minimum number of cryptographic iterations required by the system.
C. Size of the key space and the available computational power.
D. Key change methodology used by the cryptographic system.

Correct Answer: C

QUESTION 812
Which one of the following describes Kerchoff's Assumption for cryptanalytic attack?

A. Key is secret; algorithm is known.
B. Key is known; algorithm is known.
C. Key is secret; algorithm is secret.
D. Key is known; algorithm is secret.

Correct Answer: A

QUESTION 813

Which of the following actions can make a cryptographic key more resistant to an exhaustive attack?

A. None of the choices.
B. Increase the length of a key.
C. Increase the age of a key.
D. Increase the history of a key.

Correct Answer: B

QUESTION 814

Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis
B. Differential linear cryptanalysis
C. Birthday attack
D. Statistical attack

Correct Answer: C

QUESTION 815

Frame-relay uses a public switched network to provide:

A. Local Area Network (LAN) connectivity
B. Metropolitan Area Network (MAN) connectivity
C. Wide Area Network (WAN) connectivity
D. World Area Network (WAN) connectivity

Correct Answer: C

QUESTION 816

Which of the following technologies has been developed to support TCP/IP networking over low speed serial interfaces?

A. ISDN
B. SLIP
C. xDSL
D. T1

Correct Answer: B

QUESTION 817

Which of the following provide network redundancy in a local network environment?

A. Mirroring
B. Shadowing
C. Dual backbones
D. Duplexing

Correct Answer: C

QUESTION 818

Which of the following is a Wide Area Network that was originally funded by the Department of Defense, which uses TCP/IP for data interchange?

A. the Internet
B. the Intranet
C. the Extranet
D. the Ethernet

Correct Answer: A

QUESTION 819

Internet specifically refers to the global network of:

A. public networks and Internet Service Providers (ISPs) throughout the world
B. private networks and Internet Services Providers (ISPs) through the world
C. limited networks and Internet Service Providers (ISPs) throughout the world
D. point networks and Internet Service Providers (ISPs) throughout the world

Correct Answer: A

QUESTION 820

To improve the integrity of asynchronous communications in the realm of personal computers, the Microcom Networking Protocol (MNP) uses a highly effective communications error-control technique known as

A. Cyclic redundancy check
B. Vertical redundancy check