Reference(s) used for this question:

For more information and illustration on Cross certification:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx
http://www.entrust.com/resources/pdf/cross_certification.pdf

also see:
Shon Harris, CISSP All in one book, 4th Edition, Page 727
RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile; FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 254.

QUESTION 692
Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

A. Timestamping
B. Repository
C. Certificate revocation
D. Internet Key Exchange (IKE)

Correct Answer: D
Explanation:
Other elements are included in a PKI.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 165).

QUESTION 693
Which of the following is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet?

A. Secure Electronic Transaction (SET)
B. MONDEX
C. Secure Shell (SSH-2)
D. Secure Hypertext Transfer Protocol (S-HTTP)

Correct Answer: A
Explanation:
SET was developed by a consortium including Visa and MasterCard.
Source: Harris, Shon, CISSP All In One Exam Guide, pages 668-669.
Mondex is a smart card electronic cash system owned by MasterCard. SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet. Secure HTTP is a secure message-oriented communications protocol designed for use in conjunction with HTTP. It is designed to coexist with HTTP's messaging model and to be easily integrated with HTTP applications.

QUESTION 694
A one-way hash provides which of the following?

A. Confidentiality
B. Availability

C. Integrity
D. Authentication

Correct Answer: C
Explanation:
A one-way hash is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value. It provides integrity, but no confidentiality, availability or authentication.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 5).

QUESTION 695
What size is an MD5 message digest (hash)?

A. 128 bits
B. 160 bits
C. 256 bits
D. 128 bytes

Correct Answer: A
Explanation:
MD5 is a one-way hash function producing a 128-bit message digest from the input message, through 4 rounds of transformation. MD5 is specified as an Internet Standard (RFC1312).
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 696
Which of the following statements is most accurate regarding a digital signature?

A. It is a method used to encrypt confidential data.
B. It is the art of transferring handwritten signature to electronic media.
C. It allows the recipient of data to prove the source and integrity of data.
D. It can be used as a signature system and a cryptosystem.

Correct Answer: C
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 697
You work in a police department forensics lab where you examine computers for evidence of crimes. Your work is vital to the success of the prosecution of criminals. One day you receive a laptop and are part of a two man team responsible for examining it together. However, it is lunch time and after receiving the laptop you leave it on your desk and you both head out to lunch. What critical step in forensic evidence have you forgotten?

A. Chain of custody
B. Locking the laptop in your desk
C. Making a disk image for examination
D. Cracking the admin password with chntpw

Correct Answer: A
Explanation:
When evidence from a crime is to be used in the prosecution of a criminal it is critical that you follow the law when handling that evidence. Part of that process is called chain of custody and is when you maintain proactive and documented control over ALL evidence involved in a crime.

Failure to do this can lead to the dismissal of charges against a criminal because if the evidence is compromised because you failed to maintain of chain of custody.

A chain of custody is chronological documentation for evidence in a particular case, and is especially important with electronic evidence due to the possibility of fraudulent data alteration, deletion, or creation. A fully detailed chain of custody report is necessary to prove the physical custody of a piece of evidence and show all parties that had access to said evidence at any given time.

Evidence must be protected from the time it is collected until the time it is presented in court.

The following answers are incorrect:

Locking the laptop in your desk: Even this wouldn't assure that the defense team would try to challenge chain of custody handling. It's usually easy to break into a desk drawer and evidence should be stored in approved safes or other storage facility.

Making a disk image for examination: This is a key part of system forensics where we make a disk image of the evidence system and study that as opposed to studying the real disk drive. That could lead to loss of evidence. However if the original evidence is not secured than the chain of custoday has not been maintained properly.

Cracking the admin password with chntpw: This isn't correct. Your first mistake was to compromise the chain of custody of the laptop. The chntpw program is a Linux utility to (re)set the password of any user that has a valid (local) account on a Windows system, by modifying the crypted password in the registry's SAM file. You do not need to know the old password to set a new one. It works offline which means you must have physical access (i.e., you have to shutdown your computer and boot off a linux floppy disk). The bootdisk includes stuff to access NTFS partitions and scripts to glue the whole thing together. This utility works with SYSKEY and includes the option to turn it off. A bootdisk image is provided on their website at http://freecode.com/projects/chntpw .

The following reference(s) was used to create this question:

http://www.cccure.tv/
http://en.wikipedia.org/wiki/Chain_of_custody
http://www.datarecovery.com/forensic_chain_of_custody.asp
QUESTION 698
Which of the following is not an example of a block cipher?

A. Skipjack
B. IDEA
C. Blowfish
D. RC4

Correct Answer: D
Explanation:
RC4 is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data

Security, Inc. Skipjack, IDEA and Blowfish are examples of block ciphers.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 699
Which of the following is the most secure form of triple-DES encryption?

A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2

Correct Answer: A
Explanation:
Triple DES with three distinct keys is the most secure form of triple-DES encryption. It can either be DES-EEE3 (encrypt-encrypt-encrypt) or DES-EDE3 (encrypt- decrypt-encrypt). DES-EDE1 is not defined and would mean using a single key to encrypt, decrypt and encrypt again, equivalent to single DES. DES-EEE4 is not defined and DES- EDE2 uses only 2 keys (encrypt with first key, decrypt with second key, encrypt with first key again).
Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 700
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?

A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA

Correct Answer: B
Explanation:
Reference:
Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".
Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

QUESTION 701
The Diffie-Hellman algorithm is used for:

A. Encryption
B. Digital signature
C. Key agreement
D. Non-repudiation

Correct Answer: C
Explanation:
The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt and decrypt messages. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study

Guide), April 2002 (page 4).

Note:
key agreement, is different from key exchange, the functionality used by the other asymmetric algorithms.

References:
AIO, third edition Cryptography (Page 632)
AIO, fourth edition Cryptography (Page 709)

QUESTION 702
Which of the following statements pertaining to key management is incorrect?

A. The more a key is used, the shorter its lifetime should be.
B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.

Correct Answer: B
Explanation:
A key should always be using the full spectrum of the keyspace and be extremely random. Other statements are correct.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 703
Which of the following concerning the Rijndael block cipher algorithm is false?

A. The design of Rijndael was strongly influenced by the design of the block cipher Square.
B. A total of 25 combinations of key length and block length are possible
C. Both block size and key length can be extended to multiples of 64 bits.
D. The cipher has a variable block length and key length.

Correct Answer: C
Explanation:
The answer above is the correct answer because it is FALSE. Rijndael does not support multiples of 64 bits but multiples of 32 bits in the range of 128 bits to 256 bits.
Key length could be 128, 160, 192, 224, and 256.

Both block length and key length can be extended very easily to multiples of 32 bits. For a total combination of 25 different block and key size that are possible.
The Rijndael Cipher
Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen as a candidate algorithm for the Advanced Encryption Standard (AES) in the United States of America. The cipher has a variable block length and key length.

Rijndael can be implemented very efficiently on a wide range of processors and in hardware.

The design of Rijndael was strongly influenced by the design of the block cipher Square.

The Advanced Encryption Standard (AES)
The Advanced Encryption Standard (AES) keys are defined to be either 128, 192, or 256 bits in accordance with the requirements of the AES.