QUESTION 805
Which of the following statements pertaining to link encryption is false?

A. It encrypts all the data along a specific communication path.
B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Correct Answer: C
Explanation:
When using link encryption, packets have to be decrypted at each hop and encrypted again.
Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.
Link Encryption vs. End-to-End Encryption.
Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.
End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.
Reference: All in one, Page 735 & Glossary
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 806
What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service

Correct Answer: A
Explanation:
Reference: RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 807
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
Explanation:
A Birthday attack is usually applied to the probability of two different messages using the same hash function producing a common message digest.

The term "birthday" comes from the fact that in a room with 23 people, the probability of two of more people having the same birthday is greater than 50%.

Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Differential Cryptanalysis is a potent cryptanalytic technique introduced by Biham and Shamir. Differential cryptanalysis is designed for the study and attack of DES-like cryptosystems. A DES-like cryptosystem is an iterated cryptosystem which relies on conventional cryptographic techniques such as substitution and diffusion.

Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in an input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behaviour, and exploiting such properties to recover the secret key.

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 163).
http://en.wikipedia.org/wiki/Differential_cryptanalysis

QUESTION 808
What is NOT true about a one-way hashing function?

A. It provides authentication of the message
B. A hash cannot be reverse to get the message used to create the hash
C. The results of a one-way hash is a message digest
D. It provides integrity of the message

Correct Answer: A
Explanation:
A one way hashing function can only be use for the integrity of a message and not for authentication or confidentiality. Because the hash creates just a fingerprint of the message which cannot be reversed and it is also very difficult to create a second message with the same hash.
A hash by itself does not provide Authentication. It only provides a weak form or integrity. It would be possible for an attacker to perform a Man-In-The-Middle attack where both the hash and the digest could be changed without the receiver knowing it.
A hash combined with your session key will produce a Message Authentication Code (MAC) which will provide you with both authentication of the source and integrity. It is sometimes referred to as a Keyed Hash.
A hash encrypted with the sender private key produce a Digital Signature which provide authentication, but not the hash by itself.
Hashing functions by themselves such as MD5, SHA1, SHA2, SHA-3 does not provide authentication.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 548

QUESTION 809

Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?

A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys

Correct Answer: A
Explanation:
There is no DES mode call DES-EEE1. It does not exist.

The following are the correct modes for triple-DES (3DES):

DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted; DES-EDE3 uses three keys and encrypts, decrypts and encrypts data. DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

QUESTION 810
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: C
Explanation:
Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.

The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.

The following answers are incorrect:

The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.

The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.

The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).

Reference(s) used for this question:
OIG CBK Cryptography (pages 253 - 254)

QUESTION 811
The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation

Correct Answer: B
Explanation:
Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC 2631 Diffie-Hellman Key Agreement Method for more details.

In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie-Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature. Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.

NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.

KEY AGREEMENT VERSUS KEY EXCHANGE
A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.

The following answers were incorrect:

All of the other choices were not correct choices

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.google.com/patents?vid=4200770

QUESTION 812
What is the maximum number of different keys that can be used when encrypting with Triple DES?

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

Correct Answer: C
Explanation:
Triple DES encrypts a message three times. This encryption can be accomplished in several ways. The most secure form of triple DES is when the three encryptions are performed with three different keys.
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 152).

QUESTION 813
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?

A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)

Correct Answer: B
Explanation:
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers and Characteristics Standard model for network communications enables dissimilar networks to communicate, Defines 7 protocol layers (a.k.a. protocol stack) Each layer on one workstation communicates with its respective layer on another workstation using protocols (i.e. agreed-upon communication formats) "Mapping" each protocol to the model is useful for comparing protocols. Mnemonics: Please Do Not Throw Sausage Pizza Away (bottom to top layer) All People Seem To Need Data Processing (top to bottom layer).
Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 12.

QUESTION 814