Clement

The following terms are from the Software Development Security domain:

Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification below."

Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation."

The terms above are from the Software Development Security Domain.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Cryptography (Kindle Locations 227-244). . Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Cryptography (Kindle Locations 206-227). . Kindle Edition.
http://en.wikipedia.org/wiki/Verification_and_validation

QUESTION 733
Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?

A. Internet Key exchange (IKE)
B. Security Association Authentication Protocol (SAAP)
C. Simple Key-management for Internet Protocols (SKIP)
D. Key Exchange Algorithm (KEA)

Correct Answer: A
Explanation:
RFC 2828 (Internet Security Glossary) defines IKE as an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

The following are incorrect answers:

SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

The Key Exchange Algorithm (KEA) is defined as a key agreement algorithm that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the secret level by the NSA.

Security Association Authentication Protocol (SAAP) is a distracter.

Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 734

Which is NOT a suitable method for distributing certificate revocation information?

A. CA revocation mailing list
B. Delta CRL
C. OCSP (online certificate status protocol)
D. Distribution point CRL

Correct Answer: A
Explanation:
The following are incorrect answers because they are all suitable methods.

A Delta CRL is a CRL that only provides information about certificates whose statuses have changed since the issuance of a specific, previously issued CRL.

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

A Distribution point CRL or CRL Distribution Point, a location specified in the CRL Distribution Point (CRL DP) X.509, version 3, certificate extension when the certificate is issued.

References:
RFC 2459: Internet X.509 Public Key Infrastru
http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf
http://www.ipswitch.eu/online_certificate_status_protocol_en.html
Computer Security Handbook By Seymour Bosworth, Arthur E.Hutt, Michel E.Kabay
http://books.google.com/books?id=rCx5OfSFUPkC&printsec=frontcover&dq=Computer+Security+Handbook#PRA6-PA4,M1

QUESTION 735
Which of the following service is not provided by a public key infrastructure (PKI)?

A. Access control
B. Integrity
C. Authentication
D. Reliability

Correct Answer: D
Explanation:
A Public Key Infrastructure (PKI) provides confidentiality, access control, integrity, authentication and non-repudiation.
It does not provide reliability services.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 736
What kind of Encryption technology does SSL utilize?

A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)
C. Public Key
D. Private key

Correct Answer: B

Explanation:
SSL use public-key cryptography to secure session key, while the session key (secret key) is used to secure the whole session taking place between both parties communicating with each other.
The SSL protocol was originally developed by Netscape. Version 1.0 was never publicly released; version 2.0 was released in February 1995 but "contained a number of security flaws which ultimately led to the design of SSL version 3.0." SSL version 3.0, released in 1996, was a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier.
All of the other answers are incorrect.

QUESTION 737
Which of the following does NOT concern itself with key management?

A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)
D. Key Exchange Algorithm (KEA)

Correct Answer: C
Explanation:
Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

The following are all concerned with Key Management which makes them the wrong choices:
Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.

Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Diffie璈ellman key exchange (D璈) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie璈ellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Reference(s) used for this question:

Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228. It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8: Cryptography (page 713-715).
https://en.wikipedia.org/wiki/ISAKMP
http://searchsecurity.techtarget.com/definition/cryptology

QUESTION 738
Which of the following is NOT a property of the Rijndael block cipher algorithm?

A. The key sizes must be a multiple of 32 bits
B. Maximum block size is 256 bits
C. Maximum key size is 512 bits
D. The key size does not have to match the block size

Correct Answer: C
Explanation:
The above statement is NOT true and thus the correct answer. The maximum key size on Rijndael is 256 bits.

There are some differences between Rijndael and the official FIPS-197 specification for AES. Rijndael specification per se is specified with block and key sizes that must be a multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. Namely, Rijndael allows for both key and block sizes to be chosen independently from the set of { 128, 160, 192, 224, 256 } bits. (And the key size does not in fact have to match the block size).

However, FIPS-197 specifies that the block size must always be 128 bits in AES, and that the key size may be either 128, 192, or 256 bits. Therefore AES-128, AES-192, and AES- 256 are actually:
Key Size (bits) Block Size (bits)
AES-128 128 128
AES-192 192 128
AES-256 256 128

So in short:

Rijndael and AES differ only in the range of supported values for the block length and cipher key length.

For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits.

AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.

References used for this question:

http://blogs.msdn.com/b/shawnfa/archive/2006/10/09/the-differences-between-rijndael-and-aes.aspx
http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

QUESTION 739
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 certification authorities
D. Root certification authorities

Correct Answer: A
Explanation:

Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other's certificate.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 740
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?

A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure
C. Diffie-Hellman
D. DSS - Digital Signature Standard

Correct Answer: A
Explanation:
Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext (sender) and decryption of ciphertext (receiver). The keys may be identical, in practice, they represent a shared secret between two or more parties that can be used to maintain a private information link.

This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as secret key encryption. In symmetric key cryptography, each end of the conversation must have the same key or they cannot decrypt the message sent to them by the other party.

Symmetric key crypto is very fast but more difficult to manage due to the need to distribute the key in a secure means to all parts needing to decrypt the data. There is no key management built within Symmetric crypto.

PKI provides CIA - Confidentiality (Through encryption) Integrity (By guaranteeing that the message hasn't change in transit) and Authentication (Non-repudiation). Symmetric key crypto provides mostly Confidentiality.

The following answers are incorrect:

PKI - Public Key Infrastructure: This is the opposite of symmetric key crypto. Each side in PKI has their own private key and public key. What one key encrypt the other one can decrypt. You make use of the receiver public key to communicate securely with a remote user. The receiver will use their matching private key to decrypt the data.

Diffie-Hellman: Sorry, this is an asymmetric key technique. It is used for key agreement over an insecure network such as the Internet. It allows two parties who has never met to negotiate a secret key over an insecure network while preventing Man-In-The-Middle (MITM) attacks.

DSS - Digital Signature Standard: Sorry, this is an asymmetric key technique.

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

http://www.cccure.tv
http://en.wikipedia.org/wiki/Symmetric-key_algorithm

QUESTION 741