The number of rounds, or iterations of the main algorithm, can vary from 10 to 14 within the Advanced Encryption Standard (AES) and is dependent on the block size and key length. 128 bits keys uses 10 rounds or encryptions, 192 bits keys uses 12 rounds of encryption, and 256 bits keys uses 14 rounds of encryption.

The low number of rounds has been one of the main criticisms of Rijndael, but if this ever becomes a problem the number of rounds can easily be increased at little extra cost performance wise by increasing the block size and key length.

Range of key and block lengths in Rijndael and AES
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. The support for block and key lengths 160 and 224 bits was introduced in Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999 available at
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

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

Reference used for this question:

The Rijndael Page
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

QUESTION 704
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

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

Correct Answer: B
Explanation:
In cryptography, the one-time pad (OTP) is a type of encryption that is impossible to crack if used correctly. Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or pad) of the same length as the plaintext, resulting in a ciphertext. If the key is truly random, at least as long as the plaintext, never reused in whole or part, and kept secret, the ciphertext will be impossible to decrypt or break without knowing the key. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used.

First described by Frank Miller in 1882, the one-time pad was re-invented in 1917 and patented a couple of years later. It is derived from the Vernam cipher, named after Gilbert Vernam, one of its inventors. Vernam's system was a cipher that combined a message with a key read from a punched tape. In its original form, Vernam's system was vulnerable because the key tape was a loop, which was reused whenever the loop made a full cycle. One-time use came a little later when Joseph Mauborgne recognized that if the key tape were totally random, cryptanalysis would

be impossible.

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so the top sheet could be easily torn off and destroyed after use. For easy concealment, the pad was sometimes reduced to such a small size that a powerful magnifying glass was required to use it. Photos show captured KGB pads that fit in the palm of one's hand, or in a walnut shell. To increase security, one-time pads were sometimes printed onto sheets of highly flammable nitrocellulose so they could be quickly burned.

The following are incorrect answers:

A running key cipher uses articles in the physical world rather than an electronic algorithm. In classical cryptography, the running key cipher is a type of polyalphabetic substitution cipher in which a text, typically from a book, is used to provide a very long keystream. Usually, the book to be used would be agreed ahead of time, while the passage to use would be chosen randomly for each message and secretly indicated somewhere in the message.

The Running Key cipher has the same internal workings as the Vigenere cipher. The difference lies in how the key is chosen; the Vigenere cipher uses a short key that repeats, whereas the running key cipher uses a long key such as an excerpt from a book. This means the key does not repeat, making cryptanalysis more difficult. The cipher can still be broken though, as there are statistical patterns in both the key and the plaintext which can be exploited.

Steganography is a method where the very existence of the message is concealed. It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. it is sometimes referred to as Hiding in Plain Sight.

Cipher block chaining is a DES operating mode. IBM invented the cipher-block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 555).
http://en.wikipedia.org/wiki/One-time_pad
http://en.wikipedia.org/wiki/Running_key_cipher
http://en.wikipedia.org/wiki/Cipher_block_chaining#Cipher-block_chaining_.28CBC.29

QUESTION 705
Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. message non-repudiation.
B. message confidentiality.
C. message interleave checking.
D. message integrity.

Correct Answer: D
Explanation:
A keyed hash also called a MAC (message authentication code) is used for integrity protection and authenticity.

In cryptography, a message authentication code (MAC) is a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) as well as its authenticity, because only someone who knows the secret key could have modified the message.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.

HMAC
When using HMAC the symmetric key of the sender would be concatenated (added at the end) with the message. The result of this process (message + secret key) would be put through a hashing algorithm, and the result would be a MAC value. This MAC value is then appended to the message being sent. If an enemy were to intercept this message and modify it, he would not have the necessary symmetric key to create a valid MAC value. The receiver would detect the tampering because the MAC value would not be valid on the receiving side.

CBC-MAC
If a CBC-MAC is being used, the message is encrypted with a symmetric block cipher in CBC mode, and the output of the final block of ciphertext is used as the MAC. The sender does not send the encrypted version of the message, but instead sends the plaintext version and the MAC attached to the message. The receiver receives the plaintext message and encrypts it with the same symmetric block cipher in CBC mode and calculates an independent MAC value. The receiver compares the new MAC value with the MAC value sent with the message. This method does not use a hashing algorithm as does HMAC.

Cipher-Based Message Authentication Code (CMAC)
Some security issues with CBC-MAC were found and they created Cipher-Based Message Authentication Code (CMAC) as a replacement. CMAC provides the same type of data origin authentication and integrity as CBC-MAC, but is more secure mathematically. CMAC is a variation of CBC-MAC. It is approved to work with AES and Triple DES. HMAC, CBC- MAC, and CMAC work higher in the network stack and can identify not only transmission errors (accidental), but also more nefarious modifications, as in an attacker messing with a message for her own benefit. This means all of these technologies can identify intentional, unauthorized modifications and accidental changes-- three in one.

The following are all incorrect answers:

"Message non-repudiation" is incorrect.
Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a

digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

"Message confidentiality" is incorrect. The Message confidentiality is protected by encryption not by hashing algorithms.

"Message interleave checking" is incorrect. This is a nonsense term included as a distractor.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p.1384). McGraw-Hill. Kindle Edition.
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
http://searchsecurity.techtarget.com/definition/nonrepudiation
https://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 706
What key size is used by the Clipper Chip?

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

Correct Answer: D
Explanation:
The Clipper Chip is a NSA designed tamperproof chip for encrypting data and it uses the SkipJack algorithm. Each Clipper Chip has a unique serial number and a copy of the unit key is stored in the database under this serial number. The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message. It is based on a 80-bit key and a 16-bit checksum.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).

QUESTION 707
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)

Correct Answer: B
Explanation:
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it

consists of 3 "protocols"

ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.

Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.

SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.

So yes, IPSec does use IKE, but ISAKMP is part of IKE. The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.

The following are incorrect answers:

Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.

IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (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.

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

QUESTION 708
What is the effective key size of DES?

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

Correct Answer: A
Explanation:
Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the total key size was reduced to 64 bits, 56 of which make up the effective key, plus and extra 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 8: Cryptography (page 525).

QUESTION 709
In which phase of Internet Key Exchange (IKE) protocol is peer authentication performed?