depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.

KEY AGREEMENT
Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. The Diffie Hellman (DH) key agreement algorithm describes a means for two parties to agree upon a shared secret over a public network in such a way that the secret will be unavailable to eavesdroppers. The DH algorithm converts the shared secret into an arbitrary amount of keying material. The resulting keying material is used as a symmetric encryption key.

The other answers are not correct because:
DES and IDEA are both symmetric algorithms.
Diffie-Hellman is a common asymmetric algorithm, but is used only for key agreement. It is not typically used for data encryption and does not have digital signature capability.

References:
http://tools.ietf.org/html/rfc2631
For Diffie-Hellman information:
http://www.netip.com/articles/keith/diffie-helman.htm

QUESTION 761
What kind of encryption is realized in the S/MIME-standard?

A. Asymmetric encryption scheme
B. Password based encryption scheme
C. Public key based, hybrid encryption scheme
D. Elliptic curve based encryption

Correct Answer: C
Explanation:
S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and non-repudiation of electronic messages. S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages. The MIME standard therefore makes it possible to attach all types of files to e-mails.

S/MIME was originally developed by the company RSA Data Security. Ratified in July 1999 by the IETF, S/MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633.

How S/MIME works
The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.

The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.

The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message.
In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures

the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

Reference(s) used for this question:

http://en.kioskea.net/contents/139-cryptography-s-mime
RFC 2630: Cryptographic Message Syntax;
OPPLIGER, Rolf, Secure Messaging with PGP and S/MIME, 2000, Artech House; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 570;
SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 762
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session- by-session basis?

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

Correct Answer: B
Explanation:
RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:

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

SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long- term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.

IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally. Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie瓗ellman key exchange to set up a shared session secret from which cryptographic keys are derived.

The following are incorrect answers:

ISAKMP 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.
IKE is 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.
IPsec Key exchange (IKE) is only a detracto.

Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

QUESTION 763
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server

Correct Answer: B
Explanation:
Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

QUESTION 764
What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher

Correct Answer: B
Explanation:
Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.
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 134).

QUESTION 765
What is the maximum allowable key size of the Rijndael encryption algorithm?

A. 128 bits
B. 192 bits
C. 256 bits
D. 512 bits

Correct Answer: C
Explanation:
The Rijndael algorithm, chosen as the Advanced Encryption Standard (AES) to replace DES, can be categorized as an iterated block cipher with a variable block length and key length that can be independently chosen as 128, 192 or 256 bits.

Below you have a summary of the differences between AES and Rijndael. AES is the advanced encryption standard defined by FIPS 197. It is implemented differently than Rijndael:

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) Number of rounds

Block Size (bits)

AES-128

128 10 Rounds

128

AES-192

192 12 Rounds

128

AES-256

256 14 Rounds

128

Some book will say "up to 9 rounds will be done with a 128 bits keys". Really it is 10 rounds because you must include round zero which is the first round.

By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

Reference(s) used for this question:

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 153).
FIPS 197
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION 766
Which of the following ciphers is a subset on which the Vigenere polyalphabetic cipher was based

on?

A. Caesar
B. The Jefferson disks
C. Enigma
D. SIGABA

Correct Answer: A
Explanation:
In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communication security.

The following answer were incorrect:
The Jefferson disk, or wheel cipher as Thomas Jefferson named it, also known as the Bazeries Cylinder, is a cipher system using a set of wheels or disks, each with the 26 letters of the alphabet arranged around their edge. The order of the letters is different for each disk and is usually scrambled in some random way. Each disk is marked with a unique number. A hole in the centre of the disks allows them to be stacked on an axle. The disks are removable and can be mounted on the axle in any order desired. The order of the disks is the cipher key, and both sender and receiver must arrange the disks in the same predefined order. Jefferson's device had 36 disks.

An Enigma machine is any of a family of related electro-mechanical rotor cipher machines used for the encryption and decryption of secret messages. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. The early models were used commercially from the early 1920s, and adopted by military and government services of several countries. Several different Enigma models were produced, but the German military models are the ones most commonly discussed.

SIGABA: In the history of cryptography, the ECM Mark II was a cipher machine used by the United States for message encryption from World War II until the 1950s. The machine was also known as the SIGABA or Converter M-134 by the Army, or CSP-888/889 by the Navy, and a modified Navy version was termed the CSP-2900. Like many machines of the era it used an electromechanical system of rotors in order to encipher messages, but with a number of security improvements over previous designs. No successful cryptanalysis of the machine during its service lifetime is publicly known.

Reference(s) used for this question:

http://en.wikipedia.org/wiki/Jefferson_disk
http://en.wikipedia.org/wiki/Sigaba
http://en.wikipedia.org/wiki/Enigma_machine

QUESTION 767
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?