ESP is a mechanism for providing integrity and confidentiality to IP datagrams. It may also provide authentication, depending on which lgorithm and algorithm mode are used. Non-repudiation and protection from traffic analysis are not provided by ESP (RFC 1827). SSL is a secure protocol used for transmitting private information over the Internet. It works by using a public key to encrypt data that is transferred of the SSL connection. OIG 2007, page 976
SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet.

Reference(s) used for this question:

Shon Harris, CISSP All In One, 6th Edition , Page 705
RFC 1826, http://tools.ietf.org/html/rfc1826, paragraph 1.

QUESTION 781
Which of the following algorithms does NOT provide hashing?

A. SHA-1
B. MD2
C. RC4
D. MD5

Correct Answer: C
Explanation:
As it is an algorithm used for encryption and does not provide hashing functions , it is also commonly implemented ' Stream Ciphers '.

The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard (DSS). SHA was designed to be used in digital signatures and was developed when a more secure hashing algorithm was required for U.S. government applications.

MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value. It is not necessarily any weaker than the other algorithms in the "MD" family, but it is much slower.

MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break.

Reference:
Shon Harris , AIO v3 , Chapter - 8: Cryptography , Page: 644 - 645

QUESTION 782
Which of the following statements pertaining to stream ciphers is correct?

A. A stream cipher is a type of asymmetric encryption algorithm.
B. A stream cipher generates what is called a keystream.
C. A stream cipher is slower than a block cipher.
D. A stream cipher is not appropriate for hardware-based encryption.

Correct Answer: B
Explanation:
A stream cipher is a type of symmetric encryption algorithm that operates on continuous streams

of plain text and is appropriate for hardware-based encryption.

Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. A stream cipher generates what is called a keystream (a sequence of bits used as a key).

Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude Shannon in 1949. However, the keystream must be (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications.

A stream cipher makes use of a much smaller and more convenient key -- 128 bits, for example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure if it is not implemented properly as we have seen with the Wired Equivalent Privacy (WEP) protocol.

Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.
More details can be obtained on Stream Ciphers in RSA Security's FAQ on Stream Ciphers.

QUESTION 783
In a Public Key Infrastructure, how are public keys published?

A. They are sent via e-mail.
B. Through digital certificates.
C. They are sent by owners.
D. They are not published.

Correct Answer: B
Explanation:
Public keys are published through digital certificates, signed by certification authority (CA), binding the certificate to the identity of its bearer.

A bit more details:
Although "Digital Certificates" is the best (or least wrong!) in the list of answers presented, for the past decade public keys have been published (ie: made known to the World) by the means of a LDAP server or a key distribution server (ex.: http://pgp.mit.edu/). An indirect publishing method is through OCSP servers (to validate digital signatures' CRL)

Reference used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
http://technet.microsoft.com/en-us/library/dd361898.aspx

QUESTION 784
What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?

A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority

Correct Answer: B
Explanation:
A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 785
Which of the following binds a subject name to a public key value?

A. A public-key certificate
B. A public key infrastructure
C. A secret key infrastructure
D. A private key certificate

Correct Answer: A
Explanation:
Remember the term Public-Key Certificate is synonymous with Digital Certificate or Identity certificate.

The certificate itself provides the binding but it is the certificate authority who will go through the Certificate Practice Statements (CPS) actually validating the bindings and vouch for the identity of the owner of the key within the certificate.

As explained in Wikipedia:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity -- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme such as PGP or GPG, the signature is of either the user (a self-signed certificate) or other users ("endorsements") by getting people to sign each other keys. In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. RFC 2828 defines the certification authority (CA) as:

An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user's keys.

X509 Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the CPS that applies, may be responsible for the life cycle of key pairs associated with the certificates

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 786

Which of the following is defined as a key establishment protocol based on the Diffie- Hellman algorithm proposed for IPsec but superseded by IKE?

A. Diffie-Hellman Key Exchange Protocol
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY

Correct Answer: D
Explanation:
RFC 2828 (Internet Security Glossary) defines OAKLEY as 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.

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.

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

ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independant; that is, it is designed to support many different key exchanges.
Oakley and SKEME each define a method to establish an authenticated key exchange. This includes payloads construction, the information payloads carry, the order in which they are processed and how they are used.

Oakley describes a series of key exchanges-- called modes and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).

SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.

RFC 2049 describes the IKE protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI. While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.

Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and "Aggressive Mode" MUST ONLY be used in phase 1.

Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2.

References:
CISSP: Certified Information Systems Security Professional Study Guide By James Michael Stewart, Ed Tittel, Mike Chappl, page 397

RFC 2049 at: http://www.ietf.org/rfc/rfc2409
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. The All-in-one CISSP Exam Guide, 3rd Edition, by Shon Harris, page 674 The CISSP and CAP Prep Guide, Platinum Edition, by Krutz and Vines

QUESTION 787
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Correct Answer: C
Explanation:
The Internet Security Glossary (RFC2828) defines the Authority Revocation List (ARL) as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire.

Do not to confuse with an ARL with a Certificate Revocation List (CRL). A certificate revocation list is a mechanism for distributing notices of certificate revocations. The question specifically mentions "issued to CAs" which makes ARL a better answer than CRL.
http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-29.asp
$ certificate revocation list (CRL)
(I) A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were
scheduled to expire. (See: certificate expiration, X.509 certificate revocation list.)

http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-17.asp
$ authority revocation list (ARL)
(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See:
certificate expiration, X.509 authority revocation list.)

In a few words: We use CRL's for end-user cert revocation and ARL's for CA cert revocation - both can be placed in distribution points.

QUESTION 788
Which of the following is NOT a known type of Message Authentication Code (MAC)?

A. Keyed-hash message authentication code (HMAC)
B. DES-CBC
C. Signature-based MAC (SMAC)
D. Universal Hashing Based MAC (UMAC)