A. Pre Initialization Phase
B. Phase 1
C. Phase 2
D. No peer authentication is performed

Correct Answer: B
Explanation:
The Internet Key Exchange (IKE) protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IPSec can however, be configured without IKE by manually configuring the gateways communicating with each other for example. A security association (SA) is a relationship between two or more entities that describes how the entities will use security services to communicate securely.

In phase 1 of this process, IKE creates an authenticated, secure channel between the two IKE peers, called the IKE security association. The Diffie-Hellman key agreement is always performed in this phase.

In phase 2 IKE negotiates the IPSec security associations and generates the required key material for IPSec. The sender offers one or more transform sets that are used to specify an allowed combination of transforms with their respective settings.

Benefits provided by IKE include:
Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.

Allows you to specify a lifetime for the IPSec security association. Allows encryption keys to change during IPSec sessions.
Allows IPSec to provide anti-replay services.
Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation.
Allows dynamic authentication of peers.

References:
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.

Reference:
http://www.ciscopress.com/articles/article.asp?p=25474

QUESTION 710
What is the key size of the International Data Encryption Algorithm (IDEA)?

A. 64 bits
B. 128 bits
C. 160 bits
D. 192 bits

Correct Answer: B
Explanation:
The International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64 bit blocks of data with a 128-bit key. The data blocks are divided into 16 smaller blocks and each has

eight rounds of mathematical functions performed on it. It is used in the PGP encryption software. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

QUESTION 711
What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed?

A. One-way hash
B. DES
C. Transposition
D. Substitution

Correct Answer: A
Explanation:
A cryptographic hash function is a transformation that takes an input (or 'message') and returns a fixed-size string, which is called the hash value (sometimes termed a message digest, a digital fingerprint, a digest or a checksum).

The ideal hash function has three main properties - it is extremely easy to calculate a hash for any given data, it is extremely difficult or almost impossible in a practical sense to calculate a text that has a given hash, and it is extremely unlikely that two different messages, however close, will have the same hash.

Functions with these properties are used as hash functions for a variety of purposes, both within and outside cryptography. Practical applications include message integrity checks, digital signatures, authentication, and various information security applications. A hash can also act as a concise representation of the message or document from which it was computed, and allows easy indexing of duplicate or unique data files.

In various standards and applications, the two most commonly used hash functions are MD5 and SHA-1. In 2005, security flaws were identified in both of these, namely that a possible mathematical weakness might exist, indicating that a stronger hash function would be desirable. In 2007 the National Institute of Standards and Technology announced a contest to design a hash function which will be given the name SHA-3 and be the subject of a FIPS standard.

A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the hash is unable to work out the original message, but someone knowing the original message can prove the hash is created from that message, and none other. A cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable.

A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible:

finding a (previously unseen) message that matches a given digest finding "collisions", wherein two different messages have the same message digest.

An attacker who can do either of these things might, for example, use them to substitute an authorized message with an unauthorized one.

Ideally, it should not even be feasible to find two messages whose digests are substantially similar; nor would one want an attacker to be able to learn anything useful about a message given only its digest. Of course the attacker learns at least one piece of information, the digest

itself, which for instance gives the attacker the ability to recognise the same message should it occur again.

References:
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 40-41.
also see:
http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 712
What is NOT an authentication method within IKE and IPsec?

A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication

Correct Answer: A
Explanation:
CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).

After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

The following were incorrect answers:

Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.

The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.

Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.

The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.

Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect (OSI) X.500 specification.

Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.

In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.

So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.

There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.
References:

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.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.

http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

QUESTION 713
Which of the following is NOT a symmetric key algorithm?

A. Blowfish

B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B
Explanation:
Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital signature, providing the capability to generate signatures (with the use of a private key) and verify them (with the use of the corresponding public key).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 8: Cryptography (page 550).
Reference:
DSS: http://www.itl.nist.gov/fipspubs/fip186.htm.

QUESTION 714
Which of the following is a symmetric encryption algorithm?

A. RSA
B. Elliptic Curve
C. RC5
D. El Gamal

Correct Answer: C
Explanation:
RC5 is a symmetric encryption algorithm. It is a block cipher of variable block length, encrypts through integer addition, the application of a bitwise Exclusive OR (XOR), and variable rotations.
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 153).

QUESTION 715
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?

A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.

Correct Answer: B
Explanation:
If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.

The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.