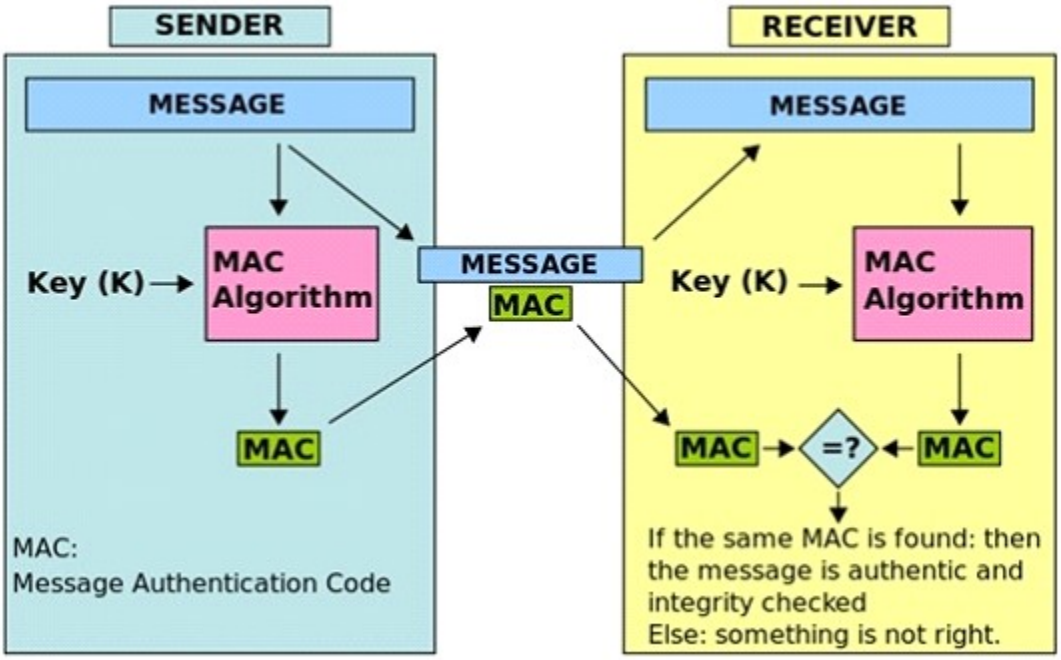
Correct Answer: C
Explanation:
There is no such thing as a Signature-Based MAC. Being the wrong choice in the list, it is the best answer to this question.

WHAT IS A Message Authentication Code (MAC)?
In Cryptography, a MAC (Message Authentication Code) also known as a cryptographic checksum, is a small block of data that is generated using a secret key and then appended to the message. When the message is received, the recipient can generate their own MAC using the secret key, and thereby know that the message has not changed either accidentally or intentionally in transit. Of course, this assurance is only as strong as the trust that the two parties have that no one else has access to the secret key. A MAC is a small representation of a message and has the following characteristics:

A MAC is much smaller than the message generating it. Given a MAC, it is impractical to compute the message that generated it. Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC.

See the graphic below from Wikipedia showing the creation of a MAC value:



Message Authentication Code MAC HMAC
In the example above, the sender of a message runs it through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag.

If they are identical, the receiver can safely assume that the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.

However, to allow the receiver to be able to detect replay attacks, the message itself must contain

data that assures that this same message can only be sent once (e.g. time stamp, sequence number or use of a one-time MAC). Otherwise an attacker could -- without even understanding its content -- record this message and play it back at a later time, producing the same result as the original sender.

NOTE:
There are many ways of producing a MAC value. Below you have a short list of some implementation.

The following were incorrect answers for this question:

They were all incorrect answers because they are all real type of MAC implementation. In the case of DES-CBC, a MAC is generated using the DES algorithm in CBC mode, and the secret DES key is shared by the sender and the receiver. The MAC is actually just the last block of ciphertext generated by the algorithm. This block of data (64 bits) is attached to the unencrypted message and transmitted to the far end. All previous blocks of encrypted data are discarded to prevent any attack on the MAC itself. The receiver can just generate his own MAC using the secret DES key he shares to ensure message integrity and authentication. He knows that the message has not changed because the chaining function of CBC would significantly alter the last block of data if any bit had changed anywhere in the message. He knows the source of the message (authentication) because only one other person holds the secret key.

A Keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5, SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.

A message authentication code based on universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message. The resulting digest or fingerprint is then encrypted to hide the identity of the hash function used. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. UMAC is specified in RFC 4418, it has provable cryptographic strength and is usually a lot less computationally intensive than other MACs.

What is the MicMac (confusion) with MIC and MAC?
The term message integrity code (MIC) is frequently substituted for the term MAC, especially in communications, where the acronym MAC traditionally stands for Media Access Control when referring to Networking. However, some authors use MIC as a distinctly different term from a MAC; in their usage of the term the MIC operation does not use secret keys. This lack of security means that any MIC intended for use gauging message integrity should be encrypted or otherwise be protected against tampering. MIC algorithms are created such that a given message will always produce the same MIC assuming the same algorithm is used to generate both. Conversely, MAC algorithms are designed to produce matching MACs only if the same message, secret key and initialization vector are input to the same algorithm. MICs do not use secret keys and, when taken on their own, are therefore a much less reliable gauge of message integrity than MACs. Because MACs use secret keys, they do not necessarily need to be encrypted to provide the same level of assurance.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 15799-15815). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Message_authentication_code
http://tools.ietf.org/html/rfc4418

QUESTION 789
Which of the following is not a disadvantage of symmetric cryptography when compared with Asymmetric Ciphers?

A. Provides Limited security services
B. Has no built in Key distribution
C. Speed
D. Large number of keys are needed

Correct Answer: C
Explanation:
Symmetric cryptography ciphers are generally fast and hard to break. So speed is one of the key advantage of Symmetric ciphers and NOT a disadvantage. Symmetric Ciphers uses simple encryption steps such as XOR, substitution, permutation, shifting columns, shifting rows, etc... Such steps does not required a large amount of processing power compare to the complex mathematical problem used within Asymmetric Ciphers.

Some of the weaknesses of Symmetric Ciphers are:
The lack of automated key distribution. Usually an Asymmetric cipher would be use to protect the symmetric key if it needs to be communicated to another entity securely over a public network. In the good old day this was done manually where it was distributed using the Floppy Net sometimes called the Sneaker Net (you run to someone's office to give them the key).

As far as the total number of keys are required to communicate securely between a large group of users, it does not scale very well. 10 users would require 45 keys for them to communicate securely with each other. If you have 1000 users then you would need almost half a million key to communicate secure. On Asymmetric ciphers there is only 2000 keys required for 1000 users. The formula to calculate the total number of keys required for a group of users who wishes to communicate securely with each others using Symmetric encryption is Total Number of Users (N) * Total Number of users minus one Divided by 2 or N (N-1)/2

Symmetric Ciphers are limited when it comes to security services, they cannot provide all of the security services provided by Asymmetric ciphers. Symmetric ciphers provides mostly confidentiality but can also provide integrity and authentication if a Message Authentication Code (MAC) is used and could also provide user authentication if Kerberos is used for example. Symmetric Ciphers cannot provide Digital Signature and Non- Repudiation.

Reference used for theis question:
WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 790
Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?

A. Message Authentication Code - MAC
B. PAM - Pluggable Authentication Module
C. NAM - Negative Acknowledgement Message

D. Digital Signature Certificate

Correct Answer: A
Explanation:
The purpose of a message authentication code - MAC is to verify both the source and message integrity without the need for additional processes.

A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

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.

In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.

The following answers are incorrect:

PAM - Pluggable Authentication Module: This isn't the right answer. There is no known message authentication function called a PAM. However, a pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes and commonly used within the Linux Operating System.

NAM - Negative Acknowledgement Message: This isn't the right answer. There is no known message authentication function called a NAM. The proper term for a negative acknowledgement is NAK, it is a signal used in digital communications to ensure that data is received with a minimum of errors.

Digital Signature Certificate: This isn't right. As it is explained and contrasted in the explanations provided above.

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

The CCCure Computer Based Tutorial for Security+, you can subscribe at
http://www.cccure.tv
http://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 791
The DES algorithm is an example of what type of cryptography?

A. Secret Key
B. Two-key
C. Asymmetric Key
D. Public Key

Correct Answer: A
Explanation:
DES is also known as a Symmetric Key or Secret Key algorithm. DES is a Symmetric Key algorithm, meaning the same key is used for encryption and decryption.

For the exam remember that:
DES key Sequence is 8 Bytes or 64 bits (8 x 8 = 64 bits) DES has an Effective key length of only 56 Bits. 8 of the Bits are used for parity purpose only.
DES has a total key length of 64 Bits.

The following answers are incorrect:

Two-key This is incorrect because DES uses the same key for encryption and decryption.

Asymmetric Key This is incorrect because DES is a Symmetric Key algorithm using the same key for encryption and decryption and an Asymmetric Key algorithm uses both a Public Key and a Private Key.

Public Key. This is incorrect because Public Key or algorithm Asymmetric Key does not use the same key is used for encryption and decryption.

References used for this question:
http://en.wikipedia.org/wiki/Data_Encryption_Standard

QUESTION 792
What is the name for a substitution cipher that shifts the alphabet by 13 places?

A. Caesar cipher
B. Polyalphabetic cipher
C. ROT13 cipher
D. Transposition cipher

Correct Answer: C
Explanation:
An extremely simple example of conventional cryptography is a substitution cipher.

A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it. So the offset could be one, two, or any number you wish. ROT-13 is an example where it is shifted 13 spaces. The Ceaser Cipher is another example where it is shifted 3 letters to the left.

ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet. ROT13 is an example of the Caesar cipher, developed in ancient Rome.

In the basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides virtually no cryptographic security, and is often cited as a canonical example of weak encryption.

ROT13 is used in online forums as a means of hiding spoilers, puzzle solutions, and offensive materials from the casual glance. ROT13 has been described as the "Usenet equivalent of a