"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed. While it is technically true that any key will eventually be broken by a brute force attack, the question remains "how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.

"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.

References:
Official ISC2 Guide page: 259
All in One Third Edition page: 623

QUESTION 716
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Explanation:
Content security measures presumes that the content is available in cleartext on the central mail server.
Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".
There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

QUESTION 717
Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?

A. Twofish
B. Serpent
C. RC6
D. Rijndael
Correct Answer: D
Explanation:
The Correct Answer: Rijndael. Rijndael is the new approved method of encrypting sensitive but unclassified information for the U.S. government. It has been accepted by and is also widely used in the public arena as well. It has low memory requirements and has been constructed to easily defend against timing attacks.

The following answers are incorrect: Twofish. Twofish was among the final candidates chosen for AES, but was not selected.

Serpent. Serpent was among the final candidates chosen for AES, but was not selected. RC6. RC6 was among the final candidates chosen for AES, but was not selected.

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

ISC2 OIG, 2007 p. 622, 629-630
Shon Harris AIO, v.3 p 247-250

QUESTION 718
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?

A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature

Correct Answer: D
Explanation:
RFC 2828 (Internet Security Glossary) defines a digital signature as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

The steps to create a Digital Signature are very simple:

1. You create a Message Digest of the message you wish to send
2. You encrypt the message digest using your Private Key which is the action of Signing
3. You send the Message along with the Digital Signature to the recipient

To validate the Digital Signature the recipient will make use of the sender Public Key. Here are the steps:

1. The receiver will decrypt the Digital Signature using the sender Publick Key producing a clear text message digest.
2. The receiver will produce his own message digest of the message received.
3. At this point the receiver will compare the two message digest (the one sent and the one produce by the receiver), if the two matches, it proves the authenticity of the message and it confirms that the message was not modified in transit validating the integrity as well. Digital Signatures provides for Authenticity and Integrity only. There is no confidentiality in place, if you wish to get confidentiality it would be needed for the sender to encrypt everything with the receiver public key as a last step before sending the message.

A Digital Envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. In simple term it is a type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead. A cryptographic hash is the result of a cryptographic hash function such as MD5, SHA-1, or SHA-2. A hash value also called a Message Digest is like a fingerprint of a message. It is used to proves integrity and ensure the message was not changed either in transit or in storage.

A Message Authentication Code (MAC) refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES or it can also be produced without using DES

by concataning the Secret Key at the end of the message (simply adding it at the end of the message) being sent and then producing a Message digest of the Message+Secret Key together. The MAC is then attached and sent along with the message but the Secret Key is NEVER sent in clear text over the network.

In cryptography, HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or 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 length in bits and on the size and quality of the cryptographic key.

There is more than one type of MAC: Meet CBC-MAC
In cryptography, a Cipher Block Chaining Message Authentication Code, abbreviated CBC- MAC, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

References:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
http://www.webopedia.com/TERM/D/digital_envelope.html
http://en.wikipedia.org/wiki/CBC-MAC

QUESTION 719
What does the directive of the European Union on Electronic Signatures deal with?

A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers

Correct Answer: C
Explanation:
Reference:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures.

QUESTION 720
Cryptography does NOT help in:

A. Detecting fraudulent insertion.
B. Detecting fraudulent deletion.
C. Detecting fraudulent modification.
D. Detecting fraudulent disclosure.

Correct Answer: D
Explanation:
Cryptography is a detective control in the fact that it allows the detection of fraudulent insertion, deletion or modification. It also is a preventive control is the fact that it prevents disclosure, but it

usually does not offers any means of detecting disclosure.
Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 721
When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:

0101 0001 Plain text

0111 0011 Key stream

0010 0010 Output

What is this cryptographic operation called?

A. Exclusive-OR
B. Bit Swapping
C. Logical-NOR
D. Decryption

Correct Answer: A
Explanation:
When we encrypt data we are basically taking the plaintext information and applying some key material or keystream and conducting something called an XOR or Exclusive-OR operation.

The symbol used for XOR is the following: This is a type of cipher known as a stream cipher.

The operation looks like this:
0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output (ciphertext)

As you can see, it's not simple addition and the XOR Operation uses something called a truth table that explains why 0+1=1 and 1+1=0.

The rules are simples, if both bits are the same the result is zero, if both bits are not the same the result is one.

The following answers are incorrect:

Bit Swapping: Incorrect. This isn't a known cryptographic operations.
Logical NOR: Sorry, this isn't correct but is where only 0+0=1. All other combinations of 1+1, 1+0 equals 0. More on NOR here.
Decryption: Sorry, this is the opposite of the process of encryption or, the process of applying the keystream to the plaintext to get the resulting encrypted text.

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

For more details on XOR and all other QUESTION NO: s of cryptography. Subscribe to our holistic Security+ CBT tutorial at
http://www.cccure.tv
http://en.wikipedia.org/wiki/Exclusive-or
http://en.wikipedia.org/wiki/Stream_cipher

QUESTION 722
What algorithm was DES derived from?

A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.

Correct Answer: D
Explanation:
NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.

The following answers are incorrect:

Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.
Skipjack. This is incorrect, Skipjack was developed after DES by the NSA.
Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

QUESTION 723
Compared to RSA, which of the following is true of Elliptic Curve Cryptography(ECC)?

A. It has been mathematically proved to be more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.

Correct Answer: D
Explanation:
The following answers are incorrect: It has been mathematically proved to be less secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.

It has been mathematically proved to be more secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.

It is believed to require longer key for equivalent security. On the contrary, it is believed to require shorter keys for equivalent security of RSA.
Shon Harris, AIO v5 pg719 states:

"In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter that what RSA requires"

The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 258
Shon Harris, AIO v5 pg719

QUESTION 724
Which of the following statements pertaining to block ciphers is incorrect?