A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Some Block ciphers can operate internally as a stream.

Correct Answer: C
Explanation:
Block ciphers do not use public cryptography (private and public keys). Block ciphers is a type of symmetric-key encryption algorithm that transforms a fixed-size block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. They are appropriate for software implementations and can operate internally as a stream. See more info below about DES in Output Feedback Mode (OFB), which makes use internally of a stream cipher.

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

Reference(s) used for this question:

Wikipedia on Block Cipher mode at:
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
http://www.itl.nist.gov/fipspubs/fip81.htm

QUESTION 725
Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C
Explanation:
In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
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 132).

QUESTION 726
In a known plaintext attack, the cryptanalyst has knowledge of which of the following?

A. the ciphertext and the key
B. the plaintext and the secret key
C. both the plaintext and the associated ciphertext of several messages
D. the plaintext and the algorithm

Correct Answer: C
Explanation:
In a known plaintext attack, the attacker has the plaintext and ciphertext of one or more messages. The goal is to discover the key used to encrypt the messages so that other messages can be deciphered and read.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 3rd Ed., chapter 8: Cryptography (page 676). Also check out: Handbook of Applied Cryptography 4th Edition by Alfred J.Menezes, Paul C.van Oorschot and Scott A.Vanstone.

QUESTION 727
What attribute is included in a X.509-certificate?

A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder

Correct Answer: A
Explanation:
RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 728
What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.

Correct Answer: A
Explanation:
A given message and key always produce the same ciphertext.

The following answers are incorrect:

Repetitive encryption obscures any repeated patterns that may have been present in the plaintext. Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces the same ciphertext

Individual characters are encoded by combining output from earlier encryption routines with plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached. This is a characteristic of Cipher Feedback. Cipher Feedback the ciphertext is run through a key-generating device to create the key for the next block of plaintext.

The previous DES output is used as input. Is incorrect because This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached . This is a characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous block to encrypt the next block.

QUESTION 729
The RSA algorithm is an example of what type of cryptography?

A. Asymmetric Key.
B. Symmetric Key.
C. Secret Key.
D. Private Key.

Correct Answer: A
Explanation:
The following answers are incorrect.
Symmetric Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Symmetric Key or a Secret Key cryptographic system.
Secret Key. Is incorrect because RSA is a Public Key or a Asymmetric Key cryptographic system and not a Secret Key or a Symmetric Key cryptographic system.
Private Key. Is incorrect because Private Key is just one part if an Asymmetric Key cryptographic system, a Private Key used alone is also called a Symmetric Key cryptographic system.

QUESTION 730
Which of the following offers confidentiality to an e-mail message?

A. The sender encrypting it with its private key.
B. The sender encrypting it with its public key.
C. The sender encrypting it with the receiver's public key.
D. The sender encrypting it with the receiver's private key.

Correct Answer: C
Explanation:
An e-mail message's confidentiality is protected when encrypted with the receiver's public key, because he is the only one able to decrypt the message. The sender is not supposed to have the receiver's private key. By encrypting a message with its private key, anybody possessing the corresponding public key would be able to read the message. By encrypting the message with its public key, not even the receiver would be able to read the message.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 8: Cryptography (page 517).

QUESTION 731
Which of the following is not a property of the Rijndael block cipher algorithm?

A. It employs a round transformation that is comprised of three layers of distinct and invertible transformations.
B. It is suited for high speed chips with no area restrictions.
C. It operates on 64-bit plaintext blocks and uses a 128 bit key.
D. It could be used on a smart card.

Correct Answer: C
Explanation:
All other properties above apply to the Rijndael algorithm, chosen as the AES standard to replace DES.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.

IDEA cipher algorithm operates on 64-bit plaintext blocks and uses a 128 bit key.

Reference(s) used for this question:

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION 732
Cryptography does not concern itself with which of the following choices?

A. Availability
B. Integrity
C. Confidentiality
D. Validation

Correct Answer: D
Explanation:
The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Unlike the other domains, cryptography does not completely support the standard of availability.
Availability
Cryptography supports all three of the core principles of information security. Many access control systems use cryptography to limit access to systems through the use of passwords. Many token-based authentication systems use cryptographic-based hash algorithms to compute one-time passwords. Denying unauthorized access prevents an attacker from entering and damaging the system or network, thereby denying access to authorized users if they damage or currupt the data.

Confidentiality
Cryptography provides confidentiality through altering or hiding a message so that ideally it cannot be understood by anyone except the intended recipient.

Integrity
Cryptographic tools provide integrity checks that allow a recipient to verify that a message has not been altered. Cryptographic tools cannot prevent a message from being altered, but they are

effective to detect either intentional or accidental modification of the message. Additional Features of Cryptographic Systems In addition to the three core principles of information security listed above, cryptographic tools provide several more benefits.

Nonrepudiation
In a trusted environment, the authentication of the origin can be provided through the simple control of the keys. The receiver has a level of assurance that the message was encrypted by the sender, and the sender has trust that the message was not altered once it was received. However, in a more stringent, less trustworthy environment, it may be necessary to provide assurance via a third party of who sent a message and that the message was indeed delivered to the right recipient. This is accomplished through the use of digital signatures and public key encryption. The use of these tools provides a level of nonrepudiation of origin that can be verified by a third party.

Once a message has been received, what is to prevent the recipient from changing the message and contesting that the altered message was the one sent by the sender? The nonrepudiation of delivery prevents a recipient from changing the message and falsely claiming that the message is in its original state. This is also accomplished through the use of public key cryptography and digital signatures and is verifiable by a trusted third party.

Authentication
Authentication is the ability to determine if someone or something is what it declares to be. This is primarily done through the control of the keys, because only those with access to the key are able to encrypt a message. This is not as strong as the nonrepudiation of origin, which will be reviewed shortly Cryptographic functions use several methods to ensure that a message has not been changed or altered. These include hash functions, digital signatures, and message authentication codes (MACs). The main concept is that the recipient is able to detect any change that has been made to a message, whether accidentally or intentionally.

Access Control
Through the use of cryptographic tools, many forms of access control are supported--from log-ins via passwords and passphrases to the prevention of access to confidential files or messages. In all cases, access would only be possible for those individuals that had access to the correct cryptographic keys.

NOTE FROM CLEMENT:
As you have seen this question was very recently updated with the latest content of the Official ISC2 Guide (OIG) to the CISSP CBK, Version 3.

Myself, I agree with most of you that cryptography does not help on the availability side and it is even the contrary sometimes if you loose the key for example. In such case you would loose access to the data and negatively impact availability. But the ISC2 is not about what I think or what you think, they have their own view of the world where they claim and state clearly that cryptography does address availability even thou it does not fully address it.

They look at crypto as the ever emcompassing tool it has become today. Where it can be use for authentication purpose for example where it would help to avoid corruption of the data through illegal access by an unauthorized user.

The question is worded this way in purpose, it is VERY specific to the CISSP exam context where ISC2 preaches that cryptography address availability even thou they state it does not fully address it. This is something new in the last edition of their book and something you must be aware of.

Best regards