Which of the following is not a DES mode of operation?

A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback

Correct Answer: C
Explanation:
Output feedback (OFB) is a DES mode of operation, not input feedback.
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 149).

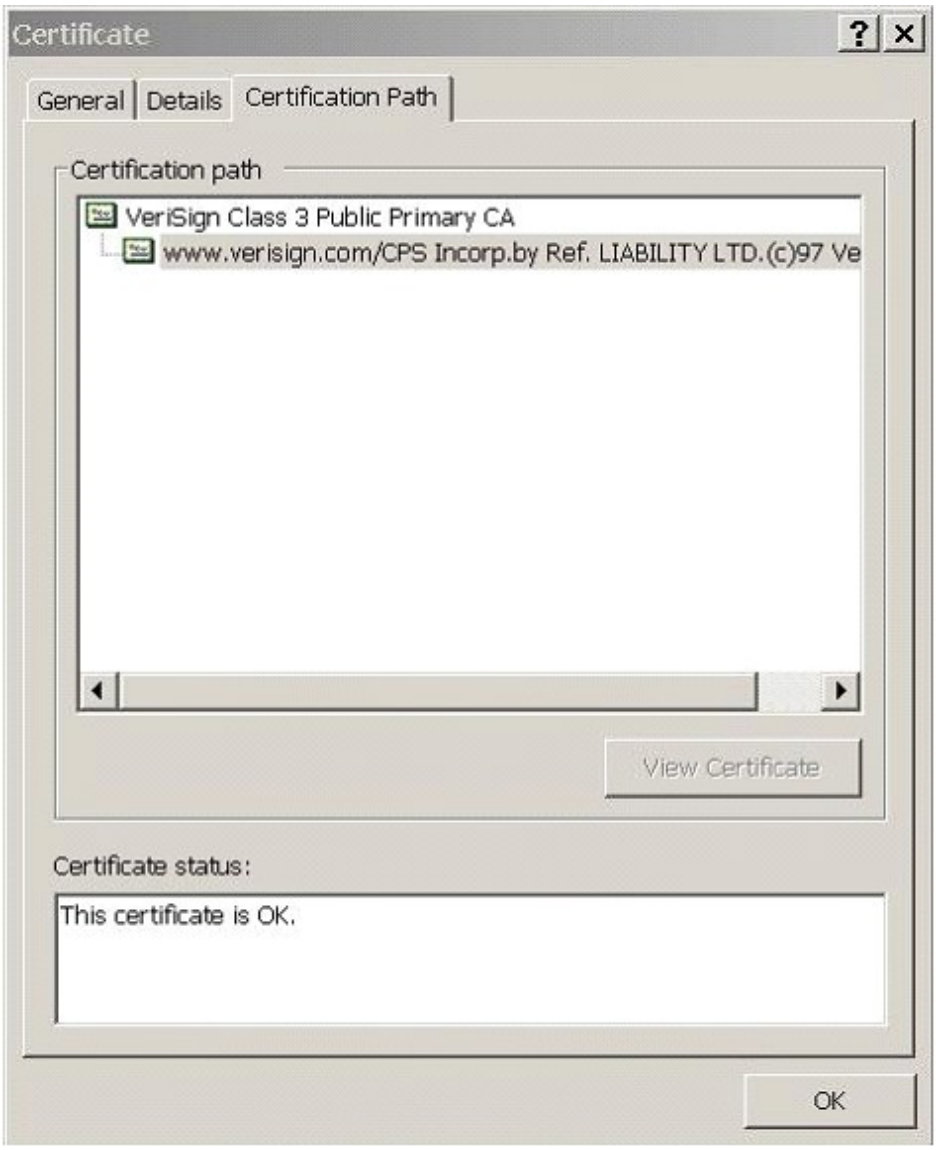
QUESTION 742
Which of the following would best describe certificate path validation?

A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate

Correct Answer: A
Explanation:
With the advent of public key cryptography (PKI), it is now possible to communicate securely with untrusted parties over the Internet without prior arrangement. One of the necessities arising from such communication is the ability to accurately verify someone's identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given entity, there should be a fool-proof method of "binding" the entity's public key to its unique domain name (DN).

A X.509 digital certificate issued by a well known certificate authority (CA), like Verisign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verifications. A X.509 certificate is a cryptographically sealed data object that contains the entity's unique DN, public key, serial number, validity period, and possibly other extensions.

The Windows Operating System offers a Certificate Viewer utility which allows you to double-click on any certificate and review its attributes in a human-readable format. For instance, the "General" tab in the Certificate Viewer Window (see below) shows who the certificate was issued to as well as the certificate's issuer, validation period and usage functions.



Certification Path graphic
The "Certification Path" tab contains the hierarchy for the chain of certificates. It allows you to select the certificate issuer or a subordinate certificate and then click on "View Certificate" to open the certificate in the Certificate Viewer.

Each end-user certificate is signed by its issuer, a trusted CA, by taking a hash value (MD5 or SHA-1) of ASN.1 DER (Distinguished Encoding Rule) encoded object and then encrypting the resulting hash with the issuer's private key (CA's Private Key) which is a digital signature. The encrypted data is stored in the "signatureValue" attribute of the entity's (CA) public certificate.

Once the certificate is signed by the issuer, a party who wishes to communicate with this entity can then take the entity's public certificate and find out who the issuer of the certificate is. Once the issuer's of the certificate (CA) is identified, it would be possible to decrypt the value of the "signatureValue" attribute in the entity's certificate using the issuer's public key to retrieve the hash value. This hash value will be compared with the independently calculated hash on the entity's certificate. If the two hash values match, then the information contained within the certificate must not have been altered and, therefore, one must trust that the CA has done

enough background check to ensure that all details in the entity's certificate are accurate.

The process of cryptographically checking the signatures of all certificates in the certificate chain is called "key chaining". An additional check that is essential to key chaining is verifying that the value of the "subjectKeyIdentifier" extension in one certificate matches the same in the subsequent certificate.

Similarly, the process of comparing the subject field of the issuer certificate to the issuer field of the subordinate certificate is called "name chaining". In this process, these values must match for each pair of adjacent certificates in the certification path in order to guarantee that the path represents unbroken chain of entities relating directly to one another and that it has no missing links.

The two steps above are the steps to validate the Certification Path by ensuring the validity of all certificates of the certificate chain to the root certificate as described in the two paragraphs above.

Reference(s) used for this question:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 262.
https://www.tibcommunity.com/docs/DOC-2197

QUESTION 743
Which of the following is best at defeating frequency analysis?

A. Substitution cipher
B. Polyalphabetic cipher
C. Transposition cipher
D. Ceasar Cipher

Correct Answer: B
Explanation:
Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis.
In every language, there are words and patterns that are used more than others.

Some patterns common to a language can actually help attackers figure out the transformation between plaintext and ciphertext, which enables them to figure out the key that was used to perform the transformation. Polyalphabetic ciphers use different alphabets to defeat frequency analysis.

The ceasar cipher is a very simple substitution cipher that can be easily defeated and it does show repeating letters.

Out of list presented, it is the Polyalphabetic cipher that would provide the best protection against simple frequency analysis attacks.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).
DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 744
How many bits is the effective length of the key of the Data Encryption Standard algorithm?

A. 168
B. 128
C. 56
D. 64

Correct Answer: C
Explanation:
The correct answer is "56". This is actually a bit of a trick question, since the actual key length is 64 bits. However, every eighth bit is ignored because it is used for parity. This makes the "effective length of the key" that the question actually asks for 56 bits.

The other answers are not correct because:

168 - This is the number of effective bits in Triple DES (56 times 3).
128 - Many encryption algorithms use 128 bit key, but not DES. Note that you may see 128 bit encryption referred to as "military strength encryption" because many military systems use key of this length.
64 - This is the actual length of a DES encryption key, but not the "effective length" of the DES key.

Reference:
Official ISC2 Guide page: 238
All in One Third Edition page: 622

QUESTION 745
Which of the following is not an encryption algorithm?

A. Skipjack
B. SHA-1
C. Twofish
D. DEA

Correct Answer: B
Explanation:
The SHA-1 is a hashing algorithm producing a 160-bit hash result from any data. It does not perform encryption.

In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard.

SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA- 0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use. NIST required many applications in federal agencies to move to SHA-2 after 2010 because of the weakness. Although no successful attacks have yet been reported on

SHA-2, they are algorithmically similar to SHA-1.

In 2012, following a long-running competition, NIST selected an additional algorithm, Keccak, for standardization as SHA-3

NOTE:
A Cryptographic Hash Function is not the same as an Encryption Algorithm even thou both are Algorithms. An algorithm is defined as a step-by-step procedure for calculations. Hashing Algorithm do not encrypt the data. People sometimes will say they encrypted a password with SHA-1 but really they simply created a Message Digest of the password using SHA-1, putting the input through a series of steps to come out with the message digest or hash value.

A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.

Encryption Algorithms are reversible but Hashing Algorithms are not meant to be reversible if the input is large enough.

The following are incorrect answers:

The Skipjack algorithm is a Type II block cipher with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level.

Twofish is a freely available 128-bit block cipher designed by Counterpane Systems (Bruce Schneier et al.).

DEA is a symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard (DES). DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

Reference(s) used for this question:

http://en.wikipedia.org/wiki/SHA-1
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
Counterpane Labs, at http://www.counterpane.com/twofish.html.

QUESTION 746
What is the length of an MD5 message digest?

A. 128 bits
B. 160 bits
C. 256 bits
D. varies depending upon the message size.

Correct Answer: A
Explanation:
A hash algorithm (alternatively, hash "function") takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash algorithm is a hash algorithm that is designed to achieve certain security properties. The Federal Information Processing Standard 180-3, Secure Hash Standard, specifies five cryptographic hash