Model Answer

Network Security (MCA- V)

Short Answer type questions:

1. SHA: Secure hash algorithm is a collection of cryptographic hash functions. SHA 1 is the fundamental 160-bit hash function. SHA-1 appears similar to the former algorithm MD5. SHA-1 was commonly used in security protocols like the PGP, TLS, SSH, and SSL.

   The second generation of the Secure Hash Algorithm is acknowledged with the label of SHA-2. This is a group of two that has functions which are alike. SHA-2 has two diverse sizes of block and these blocks are known as SHA-512 and SHA-256. SHA-3 is the latest version of SHA. It supports Hash values up to the length of 512 bits.

2. ACL: A *network access control list* is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security.

3. Nonrepudiation: Nonrepudiation is a process that prevents either sender or receiver from denying a transmitted message.

   Nonrepudiation, Origin- proof that the message was sent by the specific party.

   Nonrepudiation, destination- proof that the message was received by the specific party.

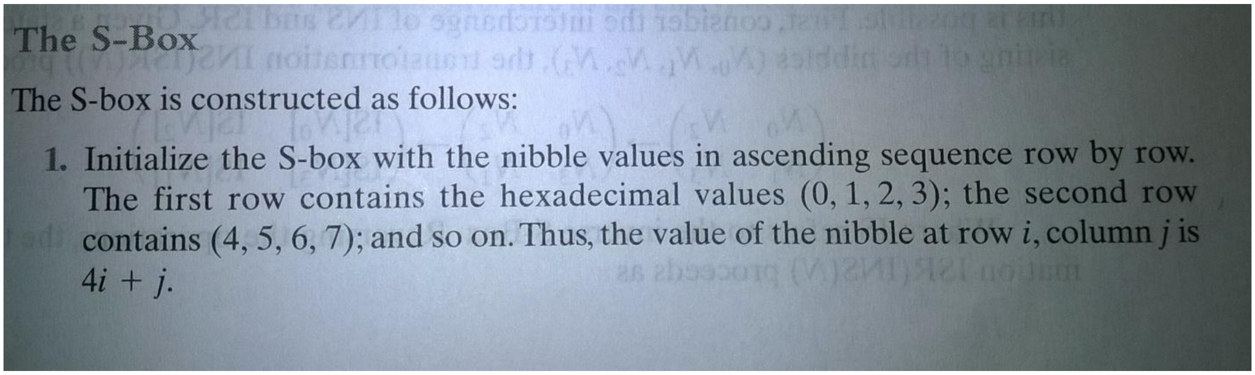
4. Answer: $X^7 + X^6 + X^5 + X^3 + X^2 + 1$

5. Iterated cryptographic hash function: Iteration of the security algorithms of hashing function for providing more security is called Iterated cryptographic hash function.

6. PGP: Pretty good privacy is the phenomenon that provides a confidentiality and authentication service that can be used for electronic mail and storage applications. It used International Data encryption algorithm standard.

7. Rail fence technique: It is the simplest transposition technique, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.
   Example: Plain text: cryptography
   c y t g a h
   r p o r p y
   Cipher text: cytgahrporpy

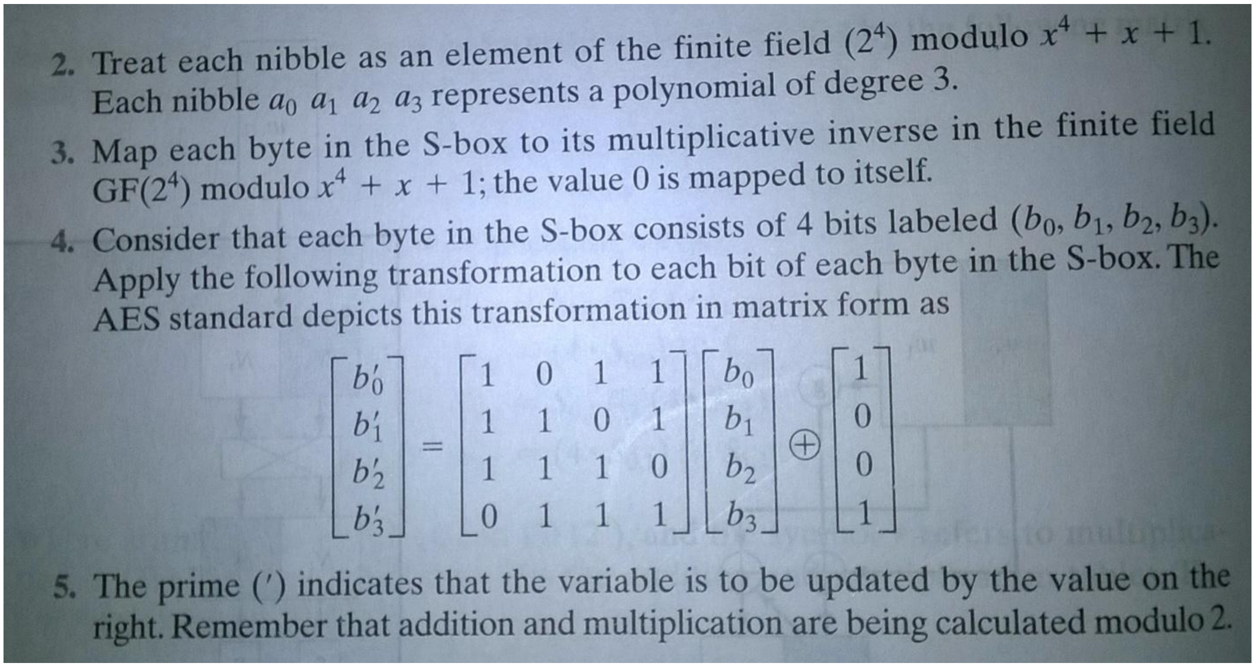
8. Linear and Non-linear S-box:



The S-Box

The S-box is constructed as follows:

1. Initialize the S-box with the nibble values in ascending sequence row by row. The first row contains the hexadecimal values (0, 1, 2, 3); the second row contains (4, 5, 6, 7); and so on. Thus, the value of the nibble at row i, column j is $4i + j$.



2. Treat each nibble as an element of the finite field (2^4) modulo $x^4 + x + 1$. Each nibble $a_0\ a_1\ a_2\ a_3$ represents a polynomial of degree 3.
3. Map each byte in the S-box to its multiplicative inverse in the finite field $GF(2^4)$ modulo $x^4 + x + 1$; the value 0 is mapped to itself.
4. Consider that each byte in the S-box consists of 4 bits labeled (b_0, b_1, b_2, b_3). Apply the following transformation to each bit of each byte in the S-box. The AES standard depicts this transformation in matrix form as

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

5. The prime (′) indicates that the variable is to be updated by the value on the right. Remember that addition and multiplication are being calculated modulo 2.

For more detail please refer *"Cryptography and Network Security, Fifth Edition by William Stallings, pp 213-214"*

9. 00100110
10. Asymmetric key cryptography: In this cryptographic system there is a key for encryption and another related key for decryption. One is called Private key, which is secret to the user only, it means no other user knows the key, and other is public key which is known to all users, stored in public key chain. For encrypting any message we use the receiver's public key and at the receiver decrypt the message using its own private key.

Long answer type questions:

1. **Define various user authentication protocol.**

Answer: Please refer *"Cryptography and Network Security, Fifth Edition by William Stallings, Chapter 15, pp 469-502"*

2. Define HASH and MAC algorithm.

Answer: Please refer *“Cryptography and Network Security, Fifth Edition by William Stallings, Chapter 11, pp 352-359, pp 393-398”*

3. Define various mathematical tools for cryptography in details.

Answer: Please refer *“Cryptography and Network Security, Fifth Edition by William Stallings, Chapter 4, pp 125-164”*

4. What are malicious software and its types in details?

Answer: You should explain the following:

a) Backdoors
b) Logic bombs
c) Viruses
d) Worms
e) Trojan Horse
f) Malwares
g) Rootkits
h) Adwares

http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

5. Define OSI security architecture in details?

Answer: You should explain these points:

a) Security attacks (Passive and active attack)
b) Security mechanisms (encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control and security label, security recovery, security audit, event detection)
c) Security services (Authentication, access control, data confidentiality, Data integrity, nonrepudiation, Availability service)

6. Define AES encryption and decryption algorithm in *detail.*

Answer: Please refer *“Cryptography and Network Security, Fifth Edition by William Stallings, Chapter 5, pp 174-202”*

7. Define Data Encryption Standard (DES) encryption and decryption algorithm in *detail.*

Answer: Please refer *“Cryptography and Network Security, Fifth Edition by William Stallings, Chapter 3, pp 101-113”*