# Symmetric Cryptography

## Learning Objective

After studying this chapter, you should be able to:

- Understanding the meaning of cryptography.
- Study the main concepts of symmetric cryptography.
- Understand symmetric encryption types, stream and block cipher.
- Present an overview of the most popular encryption algorithms, DES, 3DES, and AES.
- Understand the meaning of mode of operations.
- Realising the advantages and disadvantages of Symmetric cryptography.

# 1.Introduction

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message to be sent is called *plaintext*. The disguised message is called the *ciphertext*. In most encryption systems, the encoding and decoding depend on some *key*. Cryptanalysis is the process of deciphering a message by an unauthorised party.

Cryptographic techniques are divided into 3 types:

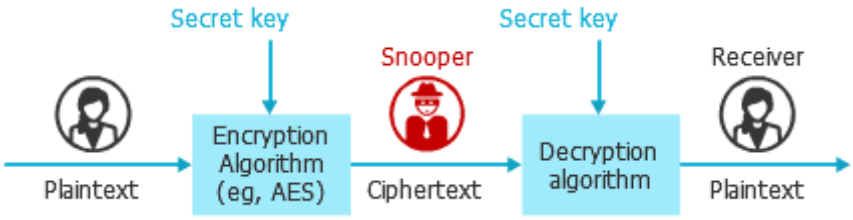
1. Symmetric-key Cryptography (divided into 2 categories).
   a) Symmetric-key ciphers (divided into 2 sub-categories)
      - Block cipher
      - Stream cipher
   b) Message Authentication Code (MACs)
2. Public-key Cryptography (divided into 2 categories).
   a) Asymmetric-key ciphers (divided into 2 sub-categories)
      - Integer Factorization
      - Discrete logarithm
   b) Signatures
3. Keyless Cryptography (also called hash functions or message digest functions).

## 2.Symmetric Encryption

Symmetric encryption, also referred to as conventional encryption, secret-key, or single-key encryption, was the only type of encryption in use prior to the development of public-key encryption in the late 1970s. It remains by far the most widely used of the two types of encryption.

To cipher a message in symmetric encryption, we write: $c = e_k(m)$ where $m$ is the plain text, $e$ is the cipher function, $k$ is the secret key, and $c$ is the cipher text

Decipherment: $m = d_k(c)$ .Typically $e$ will be public, and secrecy of $m$ (given $c$) depends totally on secrecy of $k$.




**Figure(4.1): Symmetric Encryption**

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

It is important to note that the security of symmetric encryption depends on the secrecy of the key, not the secrecy of the algorithm. That is, it is assumed that it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret, we need to keep only the key secret.

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success. As a sequence, the number of different keys for a cipher must be large.

If either type of attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there. With the exception of a scheme known as the one-time pad (described later in this chapter), there is no encryption algorithm that is unconditionally secure. Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria:

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

An encryption scheme is said to be computationally secure if either of the foregoing two criteria are met.

Symmetric-key algorithms can be divided into:

- Stream ciphers encrypt the bits of the message one at a time
- Block ciphers take a number of bits and encrypt them as a single unit

## 3.Stream Cipher

Stream ciphers are a special class of ciphers in which the encryption and decryption algorithm is applied to the individual bits or bytes of the plain-text. The algorithm works by combining the plain-text bits or bytes with a pseudo-random bit stream, one bit or byte at a time.

- A keystream is a sequence of symbols $e_1e_2e_3\ldots \in K$ (the key space for a set of encryption transformations).
- *A* an alphabet of definition of *q* symbols
- Encryption: $E_e$ is a simple substitution cipher with block length of $1$, where $e \in K, E_e = E_{e1}(m_1)E_{e2}(m_2)\ldots = c_1c_2\ldots$
  - Plaintext $m = m_1m_2\ldots(m_i \in A)$
  - Ciphertext $c = c_1c_2\ldots$
- Decryption: $D_d = D_{d1}(c_1)D_{d2}(c_2)\ldots = m_1m_2\ldots, d_i = e_i^{-1}$

The security stream ciphers depends on the changing keystream rather than the encryption function (may be simple, e.g., XOR).

A stream cipher processes the input elements continuously, producing output one element at a time as it goes along. Although block ciphers are far more common, there are certain applications in which a stream cipher is more appropriate. Stream ciphers are especially well suited for encrypting and decrypting the type of data that is used in network communication systems data in transit. Some examples of a stream cipher algorithm are the RC4 algorithm and the A5 algorithm that is used in cellular-based Global System for Mobile (GSM) communications.

### 3.1.One Time Pad

Vernam Cipher is a stream cipher defined on the alphabet $A = \{0,1\}$i.e. binary data (bits). The keystream is a binary string $(k = k_1\ldots k_t)$ of the same length as the plaintext $m(= m_1\ldots m_t)$.

- Encryption $c_i = m_i \oplus k_i$
- Decryption $m_i = c_i \oplus k_i$

Where:

$mi =$ ith binary digit of plaintext

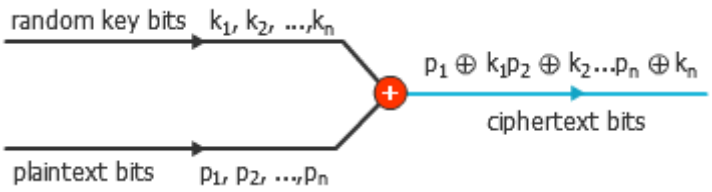
ki = ith binary digit of key

ci = ith binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation.

If the key string is randomly chosen and as long as the message and never used again, then Vernam cipher is called a one-time pad, Perfect cryptosystem. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.




**Figure(4.2): One Time Pad**

The security of the one-time pad is entirely due to the randomness of the key.

If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

In theory, we need look no further for a cipher. The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

### 3.2.Properties of Stream Ciphers

The main advantages of stream cipher are:

- Stream Ciphers have an edge over block ciphers where hardware resources are limited and less complex circuits are required like RFID tags and Smart cards.
- Stream ciphers can be useful in cases where very high speed throughput is required like multi gigabit communication channels.
- Stream ciphers are also desirable where zero error propagation is required like radio communication.
- Stream ciphers are also desirable where the length of the message cannot be predetermined and smaller input/output delay is required as in the case of GSM communication.

These are the few areas where stream ciphers have a clear edge over block ciphers due to its efficiency and speed.

The main disadvantages of stream cipher are:

The sender and receiver should be synchronized properly for correct decryption. *ie,* they must use the same key and operate on the same position (digit). If synchronization is lost due to digit insertion or deletion then re-synchronization is required. The synchronization requirement is an additional overhead that requires that both, the sender and the receiver must be properly synchronized for correct decryption. Generally if an error occurs the packet is rejected as whole and sent again.

## 4.Block Cipher

A block cipher is an encryption scheme which breaks up the plaintext message into blocks of a fixed length and produces ciphertext blocks of the same length.

In general, a symmetric block cipher consists of a sequence of rounds, with each round performing substitutions and permutations conditioned by a secret key value. The exact realization of a symmetric block cipher depends on the choice of the following parameters and design features.

- Block size: Larger block sizes mean greater security, but reduced encryption/decryption speed. A block size of 128 bits is a reasonable trade-off and is nearly universal among recent block cipher designs.
- Key size: Larger key size means greater security but may decrease encryption/ decryption speed. The most common key length in modern algorithms is 128 bits.
- Number of rounds: The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is from 10 to 16 rounds.
- Subkey generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- Round function: Again, greater complexity generally means greater resistance to cryptanalysis.

## 4.1.Symmetric Block Encryption Algorithms

The most commonly used symmetric encryption algorithms are block ciphers. A block cipher processes the plaintext input in fixed-sized blocks and produces a block of ciphertext of equal size for each plaintext block. This section focuses on the three most important symmetric block ciphers: the Data Encryption Standard (DES), triple DES (3DES), and the Advanced Encryption Standard (AES).

**Data Encryption Standard (DES)**

(DES) issued in 1977 as Federal Information Processing Standard (FIPS 46). DES uses 64 bits block in length and the key is 56 bits in length. There are 16 rounds of processing. From the original 56-bit key, 16 subkeys are generated, one of which is used for each round.

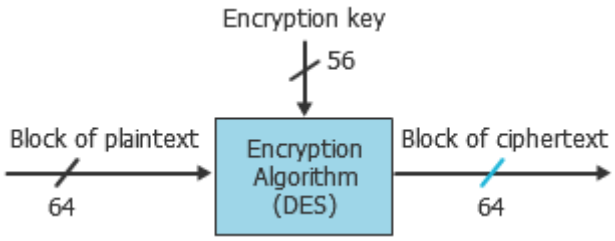
The process of decryption with DES is essentially the same as the encryption process. The rule is as follows: Use the ciphertext as input to the DES algorithm, but use the subkeys Ki in reverse order.

The strength of DES fall into two categories: concerns about the algorithm itself and concerns about the use of a 56-bit key. The first concern refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm. Over the years, there have been numerous attempts to find and exploit weaknesses in the algorithm, making DES the most studied encryption algorithm in existence.

Despite numerous approaches, no one has so far succeeded in discovering a fatal weakness in DES.

A more serious concern is key length. With a key length of $56$ bits, there are $2^{56}$ possible keys, which is approximately

$7.2 \times 10^{16}$ keys. For $80$s and $90$s computers, a brute-force attack appeared impractical. However, with current technology, the speed of commercial, off-the-shelf processors threaten the security of DES, making DES virtually worthless. For this reason DES was withdrawn in $2004$.




**Figure(4.3): DES Algorithm**

**Triple DES (3DES)**

Triple DES (3DES) was first standardized for use in financial applications in ANSI standard X9.17 in $1985$. 3DES was incorporated as part of the Data Encryption Standard in $1999$ with the publication of FIPS $46$-$3$.

3DES uses three keys and three executions of the DES algorithm. The function follows an encrypt-decrypt-encrypt (EDE) sequence:

$$C = E(K3, D(K2, E(K1, P)))$$

Where:

$C = \text{ciphertext}$ , $P = \text{plaintext}$

$E[K, X] =$ encryption of $X$ using key $K$

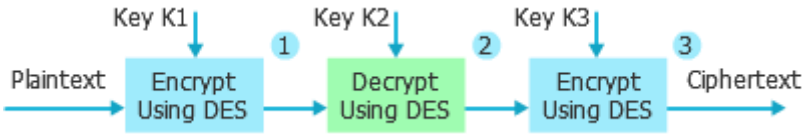
$D[K, Y] =$ decryption of $Y$ using key $K$

Decryption is simply the same operation with the keys reversed:

$$P = D(K1, E(K2, D(K3, C)))$$

With three distinct keys, 3DES has an effective key length of $168$ bits. It is easy to see that 3DES is a formidable algorithm. Because the underlying cryptographic algorithm is DES, 3DES can claim the same resistance to cryptanalysis based on

the algorithm as is claimed for DES. Furthermore, with a 168-bit key length, brute-force attacks are effectively impossible. The main disadvantage of 3DES is: it is three time slower than DES.




**Figure(4.4): 3DES algorithm**

**Advanced Encryption Standard (AES)**

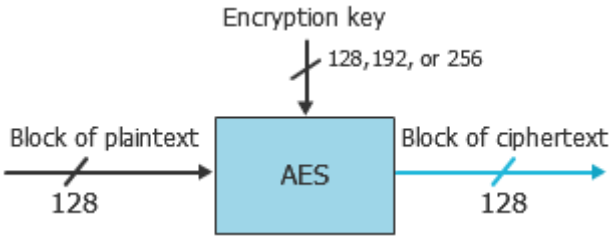
In November 2001 the USA NIST announced *Rijndael* algorithm as the AES to replace DES as a FIPS 197. AES uses a block size 128, rounds 10, 12, or 14 depending on the key size (128, 192, or 256).

The main steps of AES encryption are:

1. A plaintext of 128-bit block is arranged as a $4 \times 4$ array of bytes called the "state," which is modified in place in each round.
2. The key that is provided as input is expanded into an array of forty-four 32-bit words, w[i]. Four distinct words (128 bits) serve as a round key for each round.
3. Four different stages are used, one of permutation and three of substitution:
   - Substitute bytes: Uses a table, referred to as an S-box, to perform a byte-by-byte substitution of the block.
   - Shift rows: A simple permutation that is performed row by row.
   - Mix columns: A substitution that alters each byte in a column as a function of all of the bytes in the column.
   - Add round key: A simple bitwise XOR of the current block with a portion of the expanded key.
4. The block is copied into the State array, which is modified at each stage of encryption/decryption.
5. After the final stage the State is copied into an output matrix.

AES is the most used symmetric encryption algorithm and incorporated in a large number of commercial encryption products. The algorithm has been subjected to

extensive analysis, No flaws have been discovered. AES is modular and the key length can be extended if necessary. Similarly, the number of rounds can be increased.




**Figure(4.5): AES Algorithm**

## 5.Mode of Operation

A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used. These modes are intended for use with any symmetric block cipher, including triple DES and AES.

NIST specifies five modes of operation

1. ECB –Electronic Code Book.
2. CBC –Cipher Block Chaining.
3. CFB –Cipher FeedBack.
4. OFB –Output FeedBack.
5. CTR – Counter.

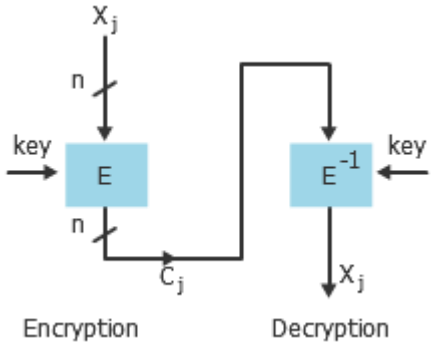
We will briefly describe the first two modes.

**Electronic Code Book (ECB)**

ECB is the simplest mode, in which plaintext is handled one block at a time and each block of plaintext is encrypted independently of other blocks. The main features of ECB are:

- Identical plaintext blocks (under the same key) result in identical ciphertext.
- Chaining dependency: blocks are enciphered independently of other blocks.

- Error propagation: one or more bit errors in a single ciphertext affect decipherment of that block only.
- ECB is not recommended for messages longer than one block, or if keys are reused for more than one-block message.
- Security of ECB may be improved by inclusion of random padding bits in each block.




**Figure(4.6): ECB Mode**

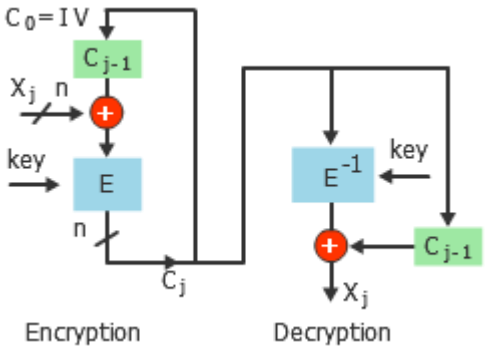
### Cipher Block Chaining (CBC)

To overcome the security deficiencies of ECB, we would like a technique in which the same plaintext block, if repeated, produces different ciphertext blocks. A simple way to satisfy this requirement is the cipher block chaining (CBC) mode. In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.

The main features of CBC are:

- Identical plaintexts blocks under the same key will yield to different ciphertext blocks.
- Chaining dependency: a ciphertext $c_j$ depends on $x_j$ and all preceding plaintext blocks $\Rightarrow$ rearranging the order of ciphertext blocks affects decryption.
- Error propagation: a single bit error in ciphertext block $c_j$ affects decipherment of $c_j$ and $c_j+1$.
- Error recovery: CBC is *self-synchronizing* in the sense that if an error occurs in block $c_j, c_j+2$ is correctly recovered.

- The initial vector $(IV)$ is not secret but needs integrity.




**Figure(4.7): CBC Mode**

## 5.1.Properties of Block Cipher

A large majority of the encryption algorithms in use at present are block ciphers. Although block ciphers are often slower than stream ciphers, they tend to be more efficient. Since block ciphers operate on larger blocks of the message at a time, they do tend to be more resource intensive and are more complex to implement in hardware or software. Block ciphers are also more sensitive to errors in the encryption process as they are working with more data. An error in the encryption process of a block cipher may render unusable a larger segment of data than what we would find in a stream cipher, as the stream cipher would only be working with 1 particular bit.

The properties of block cryptographic algorithms are not only affected by algorithm design, but also by the ways in which the algorithms are used. Different modes of operation can significantly change the properties of a block cipher. The security of block ciphers mainly depends on the complexity of the encryption function whereas thus of stream ciphers depend on the keystream randomness.

Typically, block ciphers are better for use in situations where the size of the message is fixed or known in advance, such as when we are encrypting a file or have message sizes that are reported in protocol headers. Stream ciphers are often better for use in situations where we have data of an unknown size or the data is in a continuous stream, such as we might see moving over a network.

Block cipher algorithm can be used to provide confidentiality, data integrity, or authentication, and can even be used to provide the keystream generator for stream ciphers.

## 5.2.Advantages & Disadvantages of Symmetric Encryption

The most significant advantage when it comes to the symmetric encryption method is its simplicity. As it has only one key doing encryption and decryption, symmetric encryption algorithms are considered the fastest of the two types of encryption and require less computational power to perform. This is why they are often used in situations where there is a lot of data that needs to be encrypted. Symmetric key algorithms tend to be very secure. In general, they are considered more secure than asymmetric key algorithms. In addition, exhaustive search attack, with large key size, is impossible.

However, the simplicity of symmetric encryption algorithms is not perfect. It has an issue known as “key distribution”. In the case of Bob and Alice, symmetric encryption works just fine as there are only two entities: a sender and a receiver. But what if Alice is gathering information from thousands of sources? If she gives the same key to all of her agents, every piece of data then becomes vulnerable if the key somehow gets exposed. And if Alice gives different symmetric keys to everyone, it means that she must manage thousands of keys, which isn’t a practical thing to do.

When you apply this concept to the millions of communications that take place daily between clients (web browsers) and web servers (websites), you’ll realize just how impractical that can be on a large scale.

## Exercises:

### True or False

| Question | True | False |
|---|---|---|
| 1. Symmetric encryption remains by far the most widely used of the two types of encryption. | | |
| 2. Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using different keys. It is also known as non-conventional encryption. | | |
| 3. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key. | | |
| 4. The process of converting from plaintext to ciphertext is known as deciphering or decryption. | | |
| 5. When using symmetric encryption it is very important to keep the algorithm secret. | | |
| 6. On average, half of all possible keys must be tried to achieve success with a brute-force attack. | | |
| 7. A scheme known as a one-time pad is unbreakable because it produces random output that bears no statistical relationship to the plaintext. | | |
| 8. The most widely used cipher is the Data Encryption Standard. | | |
| 9. The vast majority of network based symmetric cryptographic applications make use of stream ciphers. | | |
| 10. DES uses a 56-bit block and a 64-bit key. | | |
| 11. All other things being equal, smaller block sizes mean greater security. | | |
| 12. Greater complexity in the subkey generation algorithm should lead to greater difficulty of cryptanalysis. | | |

| | | |
|---|---|---|
| **13.** Fast software encryption/decryption and ease of analysis are two considerations in the design of a symmetric cipher. | | |
| **14.** A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length. | | |

## Multiple Choice Questions

1. An original intelligible message fed into the algorithm as input is known as _____, while the coded message produced as output is called the _____ .
   **A.** decryption, encryption
   **B.** plaintext, ciphertext
   **C.** ciphertext, plaintext
   **D.** encryption, decryption

2. Restoring the plaintext from the ciphertext is _____ .
   **A.** deciphering
   **B.** transposition
   **C.** steganography
   **D.** encryption

3. A _____ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained.
   **A.** brute-force
   **B.** Caesar attack
   **C.** ciphertext only
   **D.** chosen plaintext

4. The _____ takes the ciphertext and the secret key and produces the original plaintext. It is essentially the encryption algorithm run in reverse.
   **A.** Voronoi algorithm
   **B.** decryption algorithm
   **C.** cryptanalysis
   **D.** diagram algorithm

5. If both sender and receiver use the same key, the system is referred to as:

   **A.** public-key encryption

   **B.** two-key

   **C.** asymmetric

   **D.** conventional encryption

6. A _____ cipher is one that encrypts a digital data stream one bit or one byte at a time.

   **A.** product

   **B.** block

   **C.** key

   **D.** stream

7. A _____ cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

   **A.** bit

   **B.** product

   **C.** stream

   **D.** block

8. Key sizes of _____ or less are now considered to be inadequate.

   **A.** 128 bits

   **B.** 32 bits

   **C.** 16 bits

   **D.** 64 bits

9. One of the most intense areas of research in the field of symmetric block ciphers is _____ design.

   **A.** S-box

   **B.** F-box

   **C.** E-box

   **D.** D-box

**10.** The greater the number of rounds, the _____ it is to perform cryptanalysis.

**A.** easier

**B.** less difficult

**C.** equally difficult

**D.** harder

## References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice, 7th edn. Prentice Hall (2017).
2. Stallings, W.: Network Security essentials: application and standards, 6th edn. Pearson India Education Services Pvt. LTD (2017).
3. https://www.sciencedirect.com/topics/computer-science.

| Number of The Question | True | False |
|---|---|---|
| 1 | ✓ | |
| 2 | | ✓ |
| 3 | ✓ | |
| 4 | | ✓ |
| 5 | | ✓ |
| 6 | ✓ | |
| 7 | ✓ | |
| 8 | | ✓ |
| 9 | | ✓ |
| 10 | | ✓ |
| 11 | | ✓ |
| 12 | ✓ | |
| 13 | ✓ | |
| 14 | ✓ | |

| Number of The Question | Answer |
|---|---|
| 1 | B |
| 2 | A |
| 3 | A |
| 4 | B |
| 5 | D |
| 6 | D |
| 7 | D |
| 8 | D |
| 9 | A |
| 10 | D |