CHAPTER 2: CLASSICAL ENCRYPTION TECHNIQUES

TRUE OR FALSE

T F 1. Symmetric encryption remains by far the most widely used of the two types of encryption.

T F 2. Rotor machines are sophisticated precomputer hardware devices that use substitution techniques.

T F 3. 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.

T F 4. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

T F 5. The process of converting from plaintext to ciphertext is known as deciphering or decryption.

T F 6. The algorithm will produce a different output depending on the specific secret key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

T F 7. When using symmetric encryption it is very important to keep the algorithm secret.

T F 8. On average, half of all possible keys must be tried to achieve success with a brute-force attack.

T F 9. Ciphertext generated using a computationally secure encryption scheme is impossible for an opponent to decrypt simply because the required information is not there.

T F 10. Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

T F 11. As with Playfair, the strength of the Hill cipher is that it completely hides single letter frequencies.

T F 12. A scheme known as a one-time pad is unbreakable because it produces random output that bears no statistical relationship to the plaintext.

T F 13. The one-time pad has unlimited utility and is useful primarily for high-bandwidth channels requiring low security.

T F 14. The most widely used cipher is the Data Encryption Standard.

T F 15. Steganography renders the message unintelligible to outsiders by various transformations of the text.

MULTIPLE CHOICE

1. _____ techniques map plaintext elements (characters, bits) into ciphertext elements.

   A) Transposition B) Substitution

   C) Traditional D) Symmetric

2. Joseph Mauborgne proposed an improvement to the Vernam cipher that uses a random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) _____ .

   A) pascaline B) one-time pad

   C) polycipher D) enigma

3. 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) deciphering, enciphering D) cipher, plaintext

4. Restoring the plaintext from the ciphertext is _____ .

   A) deciphering B) transposition

   C) steganography D) encryption

5. 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

6. Techniques used for deciphering a message without any knowledge of the enciphering details is _____ .

   A) blind deciphering B) steganography

   C) cryptanalysis D) transposition

7. 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

8. 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

9. _____ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

   A) Brute-force B) Cryptanalytic

   C) Block cipher D) Transposition

10. The _____ was used as the standard field system by the British Army in World War I and was used by the U.S. Army and other Allied forces during World War II.

    A) Caesar cipher B) Playfair cipher

    C) Hill cipher D) Rail Fence cipher

11. The _____ attack is the easiest to defend against because the opponent has the least amount of information to work with.

A) ciphertext-only B) chosen ciphertext

C) known plaintext D) chosen plaintext

12. _____ refer to common two-letter combinations in the English language.

A) Streaming B) Transposition

C) Digrams D) Polyalphabetic cipher

13. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is _____ .

A) rail fence cipher B) cryptanalysis

C) polyalphabetic substitution cipher D) polyanalysis cipher

14. A technique referred to as a _____ is a mapping achieved by performing some sort of permutation on the plaintext letters.

A) transposition cipher B) polyalphabetic cipher

C) Caesar cipher D) monoalphabetic cipher

15. The methods of _____ conceal the existence of the message in a graphic image.

A) steganography B) decryptology

C) cryptology D) cryptography

SHORT ANSWER

1. _____ encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.

2. A technique for hiding a secret message within a larger document or picture in such a way that others cannot discern the presence or contents of the hidden message is _____ .

3. An encryption scheme is said to be _____ if the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

4. The two types of attack on an encryption algorithm are cryptanalysis based on properties of the encryption algorithm, and _____ which involves trying all possible keys.

5. Cryptographic systems are characterized along three independent dimensions: The type of operations used for transforming plaintext to ciphertext; The way in which the plaintext is processed; and _____ .

6. All encryption algorithms are based on two general principles: substitution and _____ .

7. One of the simplest and best known polyalphabetic ciphers is _____ cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a.

8. A _____ cipher processes the input one block of elements at a time producing an output block for each input block whereas a _____ cipher processes the input elements continuously producing output one element at a time.

9. An encryption scheme is _____ 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.

10. The earliest known and simplest use of a substitution cipher was called the _____ cipher and involved replacing each letter of the alphabet with the letter standing three places further down the alphabet.

11. The best known multiple letter encryption cipher is the _____ which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

12. The task of making large quantities of random keys on a regular basis and distributing a key of equal length to both sender and receiver for every message sent are difficulties of the _____ scheme.

13. The simplest transposition cipher is the _____ technique in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

14. The most widely used cipher ever is the _____ .

15. The _____ consist of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins with internal wiring that connects each input pin to a unique output pin.