CS 7349
Data and Network Security
Quiz #2

Name: Bingying Liang
ID: 48999397

Due: Feb 4 2024

Cryptography and Network Security: Principles and Practice, 6 th Edition, by William Stallings

CHAPTER 2: CLASSICAL ENCRYPTION TECHNIQUES

TRUE OR FALSE

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

   Solution: TRUE.

   Explanation: Symmetric encryption is commonly used because it's efficient, especially for encrypting large amounts of data.

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

   Solution: TRUE.

   Explanation: Rotor machines, like the Enigma machine used in World War II, are indeed sophisticated mechanical devices that used substitution techniques for encryption.

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.

   Solution: FALSE.

   Explanation: This describes asymmetric encryption, not symmetric. In symmetric encryption, the same key is used for both encryption and decryption.

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

Solution: TRUE.

Explanation: The biggest challenge with symmetric encryption is ensuring that the key remains secret and secure.

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

   Solution: FALSE.

   Explanation: This process is known as encryption. Deciphering or decryption is the process of converting ciphertext back into plaintext.

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.

   Solution: TRUE.

   Explanation: This is a fundamental principle of most encryption algorithms, including symmetric ones.

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

   Solution: FALSE.

   Explanation: In modern cryptography, the security of an encryption system should not depend on keeping the algorithm secret, but rather on keeping the key secret. This is known as Kerckhoffs's principle.

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

   Solution: TRUE.

   Explanation: In a brute-force attack, on average, you would need to try half of all possible keys to find the correct one.

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

   Solution: TRUE.

   Explanation: Computational security implies that the cost of breaking the cipher exceeds the value of the encrypted information or the time required is too long to be practical.

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

Solution: TRUE.

Explanation: Monoalphabetic ciphers are vulnerable to frequency analysis since each letter in the plaintext is always encrypted to the same letter in the ciphertext.

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

    Solution: TRUE.

    Explanation: Both the Playfair and Hill ciphers are polyalphabetic ciphers that conceal single letter frequencies, making them more secure against frequency analysis.

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

    Solution: TRUE.

    Explanation: The one-time pad is theoretically secure if implemented correctly, as the key is as long as the message and completely random.

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

    Solution: FALSE.

    Explanation: The one-time pad offers very high security but is impractical for many applications due to the requirement of a long, truly random key. It's not typically used for high-bandwidth channels requiring low security.

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

    Solution: FALSE.

    Explanation: The Data Encryption Standard (DES) has largely been superseded by more secure algorithms like the Advanced Encryption Standard (AES).

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

    Solution: FALSE.

    Explanation: Steganography involves hiding the existence of a message, not transforming the text to make it unintelligible. Encryption makes a message unintelligible, not steganography.

MULTIPLE CHOICE

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

   A) Transposition
   B) Substitution
   C) Traditional
   D) Symmetric

   Solution: B

   Explanation: Substitution techniques replace plaintext elements with ciphertext elements. In contrast, transposition techniques rearrange the elements without replacing them, and symmetric encryption refers to a type of encryption where the same key is used for both encryption and decryption, not a method of mapping elements. Traditional is a generic term and not specifically related to mapping elements in cryptography.

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

   Solution: B

   Explanation: The one-time pad is a cipher that uses a random key of the same length as the message, making it theoretically unbreakable. This is not characteristic of the pascaline, polycipher, or enigma. The pascaline is an early mechanical calculator, a polycipher involves multiple cipher alphabets, and the enigma was a specific rotor machine used by Germany during World War II.

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, ciphertex
   C) deciphering, enciphering
   D) cipher, plaintext

   Solution: B

   Explanation: In cryptography, the original message is known as plaintext, and the encrypted form is called ciphertext. Decryption and encryption are processes, not the names of the message forms. Deciphering and enciphering are also processes. Cipher and plaintext as pairings are incorrect because cipher is a general term for encryption methods, not a name for an encrypted message.

4. Restoring the plaintext from the ciphertext is _____.

   A) deciphering
   B) transposition
   C) steganography
   D) encryption

   Solution: A

   Explanation: Deciphering is the process of converting ciphertext back into plaintext. Transposition is a method of encryption where elements in the plaintext are rearranged. Steganography is the practice of hiding a message within another medium, not a process of restoring plaintext. Encryption is the process of converting plaintext into ciphertext, not the other way around.

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

   Solution: A

   Explanation: A brute-force attack involves trying every possible key until the right one is found. A Caesar attack (not a standard term in cryptography), ciphertext-only attack, and chosen plaintext attack are different types of cryptographic attacks, each with distinct methodologies and not specifically involving trying every possible key.

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

   A) blind deciphering
   B) steganography
   C) cryptanalysis
   D) transposition

   Solution: C

   Explanation: Cryptanalysis is the study of analyzing information systems to understand hidden aspects of the systems. It's not blind deciphering, which is not a standard term. Steganography is a method of hiding messages, not a technique for deciphering them. Transposition is an encryption method, not a technique for deciphering without knowledge of the enciphering details.

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

Solution: B

Explanation: A decryption algorithm is used to convert ciphertext back to plaintext using the secret key. The Voronoi algorithm, cryptanalysis, and diagram algorithm are not relevant to this process. The Voronoi algorithm is related to geometry, cryptanalysis is the study of breaking cryptographic systems, and the diagram algorithm isn't a standard term in cryptography.

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

Solution: D

Explanation: Conventional encryption, also known as symmetric encryption, involves using the same key for both encryption and decryption. Public-key encryption and asymmetric refer to encryption systems where different keys are used for encryption and decryption. Two-key is not a standard term in cryptography.

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

Solution: B

Explanation: Cryptanalytic attacks are those that use the nature of the encryption algorithm to try and break the cipher. Brute-force attacks are about trying all possible keys, block cipher refers to a type of encryption algorithm, and transposition is a method of encryption, not a type of attack.

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

Solution: B

Explanation: The Playfair cipher was indeed used by the British Army in World War I and the U.S. Army and other Allied forces in World War II. The Caesar cipher, Hill cipher, and Rail Fence cipher are different cryptographic algorithms and were not specifically known for this historical use.

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

Solution: A

Explanation: In a ciphertext-only attack, the attacker has the least amount of information, making it generally the easiest to defend against. Chosen ciphertext, known plaintext, and chosen plaintext attacks provide the attacker with more information or leverage, making them potentially more effective.

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

    A) Streaming
    B) Transposition
    C) Digrams
    D) Polyalphabetic cipher

Solution: C

Explanation: Digrams refer to pairs of letters in a language. Streaming, transposition, and polyalphabetic cipher are all unrelated to two-letter combinations. Streaming is related to continuous data processing, transposition is a method of encryption, and polyalphabetic cipher is a type of cipher using multiple alphabets.

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

Solution: C

Explanation: The polyalphabetic substitution cipher uses multiple cipher alphabets to encrypt the plaintext, making it more secure against frequency analysis. The rail fence cipher is a form of transposition cipher, cryptanalysis is the practice of analyzing and breaking cryptographic systems, and polyanalysis cipher is not a recognized term in cryptography.

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

Solution: A

Explanation: A transposition cipher involves rearranging the letters of the plaintext to create the ciphertext, essentially permuting the plaintext letters. A polyalphabetic cipher uses multiple alphabets to encrypt the message, a Caesar cipher shifts letters by a fixed number in the alphabet, and a monoalphabetic cipher replaces each letter with a different letter using a single fixed alphabet.

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

A) steganography B) decryptology

C) cryptology D) cryptography

Solution: A

Explanation: Steganography is the practice of hiding a message within another medium, such as a graphic image, so that the existence of the message is concealed. Decryptology is not a standard term, cryptology is the study of codes, and cryptography is the practice of creating codes, none of which are specifically about hiding messages within images.

SHORT ANSWER

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

Solution: Symmetric

Explanation: In symmetric encryption, the same key is used for both encryption and decryption. This contrasts with asymmetric encryption, where different keys are used for these processes.

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 Steganography .

Solution: Steganography

Explanation: Steganography is the technique of hiding secret messages within a larger, non-secret document, image, or another medium, in such a way that the existence of the hidden message is not apparent.

3. An encryption scheme is said to be computationally secure. 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.

   Solution: Computationally secure

   Explanation: An encryption scheme is computationally secure if the cost (in terms of resources and time) of breaking the cipher is greater than the value of the encrypted information and if 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 Brute-force attack which involves trying all possible keys.

   Solution: Brute-force attack

   Explanation: Besides cryptanalysis, the other main type of attack on an encryption algorithm is a brute-force attack, which involves trying all possible keys until the correct one is found.

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 The number of keys used.

   Solution: The number of keys used

   Explanation: Cryptographic systems are characterized by the type of operations used (substitution, transposition), the way plaintext is processed (block or stream), and the number of keys used (symmetric or asymmetric).

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

   Solution: Transposition

   Explanation: All encryption algorithms are based on two general principles: substitution, which replaces elements of the plaintext, and transposition, which rearranges the elements in the plaintext.

7. One of the simplest and best known polyalphabetic ciphers is Vigenère 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.

   Solution: Vigenère

   Explanation: The Vigenère cipher is a simple and well-known polyalphabetic cipher. It uses 26 Caesar ciphers with shifts from 0 to 25, where each cipher's key is indicated by a letter representing the shift of the letter 'a'.

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

   Solution: Block cipher, stream cipher

   Explanation: A block cipher processes the input one block of elements at a time, producing an output block for each input block. In contrast, a stream cipher processes the input elements continuously, producing output one element at a time.

9. An encryption scheme is unconditionally secure 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.

   Solution: Unconditionally secure

   Explanation: An encryption scheme is unconditionally secure if the ciphertext does not contain enough information to determine uniquely the corresponding plaintext, regardless of how much ciphertext is available.

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

    Solution: Caesar

    Explanation: The Caesar cipher is the earliest known substitution cipher and involves replacing each letter of the alphabet with the letter three positions further down.

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

    Solution: Playfair

    Explanation: The Playfair cipher is the best-known multiple-letter encryption cipher. It 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 one-time pad scheme.

    Solution: One-time pad

    Explanation: The difficulties of generating and distributing keys of equal length to both sender and receiver for each message sent are inherent to the one-time pad scheme, which requires a different key for each message.

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

    Solution: Rail Fence

    Explanation: The simplest transposition cipher is the Rail Fence technique, where plaintext is written as a sequence of diagonals and then read off as rows.

14. The most widely used cipher ever is the __Data Encryption Standard (DES)__.

    Solution: Data Encryption Standard (DES) or Advanced Encryption Standard (AES)

    Explanation: The Data Encryption Standard (DES) was historically the most widely used cipher, but it has largely been superseded by the Advanced Encryption Standard (AES), which is now the most widely used cipher.

15. The __rotor machines__ 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.

    Solution: Rotor machines

    Explanation: Rotor machines consist of a set of rotating cylinders (rotors) through which electrical pulses flow, with each rotor having 26 input and 26 output pins connected uniquely, enabling complex encryption and decryption processes.