CS 7349
Data and Network Security
Quiz #3

Name: Bingying Liang
ID: 48999397

Due: Feb 12 2024

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

CHAPTER 3: BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD

TRUE OR FALSE

1. The vast majority of network based symmetric cryptographic applications make use of stream ciphers.

   Solution: False.

   Explanation: The vast majority of network-based symmetric cryptographic applications actually make use of block ciphers, not stream ciphers. Block ciphers, like AES, are more commonly used due to their structure and security features.

2. The Feistel cipher structure, based on Shannon's proposal of 1945, dates back over a quarter of a century and is the structure used by many significant symmetric block ciphers currently in use.

   Solution: True.

   Explanation: The Feistel cipher structure, indeed based on Shannon's concept of confusion and diffusion from 1945, has been a foundation for many significant symmetric block ciphers, including DES and its successors.

3. DES uses a 56-bit block and a 64-bit key.

   Solution: False.

   Explanation: DES uses a 64-bit block size and a 64-bit key, out of which 56 bits are actually used for encryption, and 8 bits are used for parity, making the effective key size 56 bits.

4. If the bit-stream generator is a key-controlled algorithm the two users only need to share the generating key and then each can produce the keystream.

   Solution: True

   Explanation: In stream cipher applications where the bit-stream generator is key-controlled, sharing the generating key between users allows each to produce the same keystream for encryption and decryption.

5. A problem with the ideal block cipher using a small block size is that it is vulnerable to a statistical analysis of the plaintext.

   Solution: False.

   Explanation: A small block size in an ideal block cipher is not specifically vulnerable to statistical analysis; rather, the concern with small block sizes is that they may be more susceptible to certain types of attacks, such as exhaustive search attacks, because of the limited number of possible plaintext-ciphertext mappings.

6. Confusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

   Solution: True.

   Explanation: Confusion is indeed aimed at complicating the statistical relationship between plaintext and ciphertext to hinder key deduction efforts.

7. All other things being equal, smaller block sizes mean greater security.

   Solution: False.

   Explanation: Generally, larger block sizes are considered more secure because they offer more potential plaintext-ciphertext combinations, making analysis and certain types of attacks more difficult.

8. Greater complexity in the subkey generation algorithm should lead to greater difficulty of cryptanalysis.

   Solution: True.

   Explanation: Greater complexity in subkey generation contributes to the difficulty of cryptanalysis by making the relationship between the cipher key and the ciphertext more complex.

9. Fast software encryption/decryption and ease of analysis are two considerations in the design of a Feistel cipher.

Solution: False.

Explanation: Fast software encryption/decryption and ease of analysis may be considerations in cipher design, but ease of analysis refers to analysis by the cipher's designers for security evaluation, not ease for attackers. The primary considerations for a Feistel cipher include security, speed, and simplicity of design.

10. A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length.

    Solution: True.

    Explanation: The key length of DES has been a prime concern, making it vulnerable to brute-force attacks, especially as computing power has increased over time.

11. One criteria for an S-box is: "If two inputs to an S-box differ in exactly one bit, the outputs must also differ in exactly one bit. "

    Solution: False.

    Explanation: The criterion described is incorrect. A desirable property of S-boxes is that a small change in the input produces a significant and unpredictable change in the output, not a change that mirrors the input difference.

12. The heart of a Feistel block cipher is the function F, which relies on the use of S-boxes.

    Solution: True.

    Explanation: The function F in a Feistel block cipher is crucial, and while it may involve S-boxes among other elements, the statement broadly captures the importance of the function F.

13. The strict avalanche criterion and the bit independence criterion appear to weaken the effectiveness of the confusion function.

    Solution: False.

    Explanation: The strict avalanche criterion and the bit independence criterion are designed to strengthen the effectiveness of the confusion function by ensuring that a change in a single input bit affects many output bits in unpredictable ways.

14. An advantage of key-dependent S-boxes is that because they are not fixed, it is impossible to analyze the S-boxes ahead of time to look for weaknesses.

    Solution: True.

    Explanation: Key-dependent S-boxes can increase security by making pre-analysis for vulnerabilities more difficult since the S-boxes change with the key.

15. The key schedule algorithm is more popular and has received more attention than S-box design.

    Solution: False.

    Explanation: Both the key schedule algorithm and S-box design are critical in cipher design, but there is no clear evidence that one has received more attention over the other; both aspects are crucial for security.

MULTIPLE CHOICE

1. DES exhibits the classic _____ block cipher structure, which consists of a number of identical rounds of processing.

    A) Feistel B) SAC

    C) Shannon D) Rendell

    Solution: A

    Explanation: DES exhibits the classic Feistel block cipher structure, which consists of a number of identical rounds of processing. The Feistel structure allows for easy decryption and encryption with the same algorithm, only requiring the subkeys to be applied in reverse order.

2. A sequence of plaintext elements is replaced by a _____. of that sequence which means that no elements are added, deleted or replaced in the sequence, but rather the order in which the elements appear in the sequence is changed.

    A) permutation B) diffusion

    C) stream D) substitution

    Solution: A

    Explanation: A permutation in cryptographic terms means rearranging the order of elements in a sequence without adding, deleting, or replacing elements. This is fundamental in many cryptographic algorithms to achieve diffusion.

3. 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

    Solution: D

    Explanation: A stream cipher encrypts digital data one bit or byte at a time, as opposed to block ciphers, which encrypt data in larger blocks.

4. The vast majority of network-based symmetric cryptographic applications make use of _____ciphers.

   A) linear
   B) block
   C) permutation
   D) stream

   Solution: B

   Explanation: The vast majority of network-based symmetric cryptographic applications make use of block ciphers due to their efficiency in encrypting bulk data and their strong security properties.

5. 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

   Solution: D

   Explanation: A block cipher treats a block of plaintext as a whole to produce a ciphertext block of equal length, ensuring a structured, secure transformation of data.

6. _____ is when each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

   A) Substitution
   B) Diffusion
   C) Streaming
   D) Permutation

   Solution: A

   Explanation: Substitution involves replacing each plaintext element or group of elements with a corresponding ciphertext element or group of elements, a basic principle of many encryption algorithms for achieving confusion.

7. Key sizes of _____ or less are now considered to be inadequate. A)

   A) 128 bits
   B) 32 bits
   C) 16 bits
   D) 64 bits

   Solution: D

   Explanation: Key sizes of 64 bits or less are now considered inadequate due to advancements in computational power, making them vulnerable to brute-force attacks.

8. Feistel proposed that we can approximate the ideal block cipher by utilizing the concept of a _____ cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

A) linear B) permutation

C) differential D) product

Solution: D

Explanation: Feistel proposed the concept of a product cipher, which executes two or more simple ciphers in sequence to achieve a result that is cryptographically stronger than any of the component ciphers.

9. The criteria used in the design of the _____ focused on the design of the S-boxes and on the P function that takes the output of the S-boxes.

A) Avalanche Attack B) Data Encryption Standard

C) Product Cipher D) Substitution Key

Solution: B

Explanation: The criteria used in the design of the Data Encryption Standard (DES) focused heavily on the design of the S-boxes and the permutation function (P function) that processes the output of the S-boxes to ensure diffusion and confusion.

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

A) easier B) less difficult

C) equally difficult D) harder

Solution: D

Explanation: The greater the number of rounds in a cipher, the more difficult it is to perform cryptanalysis because each round adds complexity and security by further scrambling the data.

11. The function F provides the element of _____ in a Feistel cipher.

A) clarification B) alignment

C) confusion D) stability

Solution: C

Explanation: In a Feistel cipher, the function F provides the element of confusion by making the relationship between the plaintext and the ciphertext as complex as possible.

12. 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

    Solution: A

    Explanation: The design of S-boxes (Substitution-boxes) is a critical area of research in symmetric block ciphers because they are fundamental to achieving confusion within the cipher.

13. Mister and Adams proposed that all linear combinations of S-box columns should be _____ which are a special class of Boolean functions that are highly nonlinear according to certain mathematical criteria.

    A) horizontal functions B) angular functions

    C) bent functions D) vertical functions

    Solution: C

    Explanation: Bent functions are highly nonlinear Boolean functions that are desirable in the design of S-boxes because they contribute to the cipher's resistance to linear and differential cryptanalysis.

14. The Nyberg approach that is more or less a manual approach with only simple mathematics to support it is _____.

    A) human-made B) random

    C) math-made D) random with testing

    Solution: B

    Explanation: The Nyberg approach emphasizes a somewhat intuitive, manual approach to cipher design, relying on simple mathematical principles and testing rather than purely theoretical or algorithmic methods.

15. Allowing for the maximum number of possible encryption mappings from the plaintext block is referred to by Feistel as the _____.

A) ideal substitution cipher B) round function

C) ideal block cipher D) diffusion cipher

Solution: C

Explanation: Feistel referred to the concept of allowing for the maximum number of possible encryption mappings from the plaintext block as the ideal block cipher, emphasizing the goal of maximizing security through complexity and unpredictability.

SHORT ANSWER

1. A Block cipher is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

   Solution: Block cipher

   Explanation: A block cipher is an encryption scheme where a fixed-size block of plaintext is encrypted into a block of ciphertext of the same size, allowing for secure and efficient processing of large amounts of data.

2. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible so that even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex it is difficult to deduce the key.

   Solution: Confusion

   Explanation: Confusion seeks to obfuscate the relationship between the ciphertext and the encryption key, making it difficult for attackers to deduce the key even if they can analyze the ciphertext's statistics.

3. Many block ciphers have a Feistel structure structure which consists of a number of identical rounds of processing and in each round a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves.

   Solution: Feistel structure

   Explanation: The Feistel structure is a symmetric block cipher structure characterized by a series of identical rounds of processing. It alternates between substitution and permutation steps, ensuring both confusion and diffusion.

4. Feistel's is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and Diffusion functions.

   Solution: Diffusion

   Explanation: In the context of Claude Shannon's proposals, diffusion complements confusion by ensuring that the influence of plaintext or key bits is spread over many ciphertext bits, making the cipher more resistant to statistical analysis.

5. The Strict Avalanche Criterion (SAC) criterion is defined as: "An S-box satisfies GA of order y if, for a 1-bit input change, at least y output bits change."

   Solution: Strict Avalanche Criterion (SAC)

   Explanation: The SAC dictates that a change in a single input bit should result in changes in multiple output bits, ensuring that the cipher's output is highly sensitive to changes in the input, contributing to the cipher's overall security.

6. In Diffusion the statistical structure of the plaintext is dissipated into long- range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.

   Solution: Diffusion

   Explanation: Diffusion disperses the statistical structure of the plaintext across the ciphertext, ensuring that each plaintext bit affects many ciphertext bits, which enhances security by making patterns less recognizable.

7. The most widely used encryption scheme is based on the DES (Data Encryption Standard) adopted in 1977 by the National Bureau of Standards as Federal Information Processing Standard 46.

   Solution: DES (Data Encryption Standard)

   Explanation: Adopted in 1977, DES has been one of the most widely used symmetric encryption algorithms. Despite concerns over its key length, it set the foundation for modern cryptographic applications.

8. A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the Avalanche effect effect.

   Solution: Avalanche effect

   Explanation: The avalanche effect refers to the desirable property of encryption algorithms where a small change in the plaintext or key produces a significant change in the ciphertext, enhancing security by making the output unpredictable.

9. Two areas of concern regarding the level of security provided by DES are the nature of the algorithm and the Key length

   Solution: Key length

   Explanation: Concerns regarding DES's security level primarily relate to its key length. Shorter key lengths are more susceptible to brute-force attacks, making DES's 56-bit key a subject of security concerns.

10. A Timing attack attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.

Solution: Timing attack

Explanation: A timing attack exploits variations in the time it takes to encrypt or decrypt messages, which can potentially reveal information about the encryption key or algorithm's operations.

11. The Bit Independence Criterion (BIC) criterion states that output bits j and k should change independently when any single input bit i is inverted for all i, j and k.

    Solution: Explanation: The BIC states that changes in individual input bits should lead to independent changes in multiple output bits, reinforcing the cipher's resistance to various forms of cryptanalysis by ensuring high non-linearity.

12. The Feistel cipher structure cipher structure, which dates back over a quarter century and which, in turn, is based on Shannon's proposal of 1945, is the structure used by many significant symmetric block ciphers currently in use.

    Solution: Feistel cipher structure

    Explanation: This structure, inspired by Shannon's work, has been foundational in the development of many block ciphers, balancing ease of implementation with strong security through its use of substitution and permutation operations.

13. The cryptographic strength of a Feistel cipher derives from three aspects of the design: the function F, the key schedule algorithm, and Complexity and non-linearity of S-boxes, and overall design.

    Solution: Complexity and non-linearity of S-boxes, and overall design

    Explanation: The cryptographic strength of a Feistel cipher comes from its function F, key schedule algorithm, and the design of its S-boxes, which together ensure the cipher's effectiveness against attacks.

14. The Strict Avalanche Criterion (SAC) criterion states that any output bit j of an S-box should change with probability 1/2 when any single input bit i is inverted for all i,j.

    Solution: Strict Avalanche Criterion (SAC)

    Explanation: The SAC is a measure of how an encryption algorithm's output changes in response to a change in a single input bit, aiming for a 50

15. Two alternatives to DES are AES and Triple DES (3DES) DES.

    Solution: Triple DES (3DES)

    Explanation: As an alternative to DES, Triple DES applies DES encryption three times with different keys, significantly increasing security by effectively lengthening the key size and countering many of the vulnerabilities of DES.