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

CHAPTER 6: BLOCK CIPHER OPERATION

TRUE OR FALSE

T F 1. Once the plaintext is converted to ciphertext using the encryption algorithm the plaintext is then used as input and the algorithm is applied again.

T F 2. There are no practical cryptanalytic attacks on 3DES.

T F 3. A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application.

T F 4. The XTS-AES standard describes a method of decryption for data stored in sector-based devices where the threat model includes possible access to stored data by the adversary.

T F 5. S-AES is the most widely used multiple encryption scheme.

T F 6. Given the potential vulnerability of DES to a brute-force attack, an alternative has been found.

T F 7. A number of Internet based applications have adopted two-key 3DES, including PGP and S/MIME.

T F 8. The sender is the only one who needs to know an initialization vector.

T F 9. A typical application of Output Feedback mode is stream oriented transmission over noisy channel, such as satellite communication.

T F 10. Cipher Feedback (CFB) is used for the secure transmission of single values.

T F 11. Cipher Block Chaining is a simple way to satisfy the security deficiencies of ECB.

T F 12. It is possible to convert a block cipher into a stream cipher using cipher feedback, output feedback and counter modes.

T F 13. Cipher Feedback Mode conforms to the typical construction of a stream cipher.

T F 14. OFB mode requires an initialization vector that must be unique to each execution of the encryption operation.

T F 15. The XTS-AES mode is based on the concept of a tweakable block cipher.

MULTIPLE CHOICE

1. In the first instance of multiple encryption plaintext is converted to _________ using the encryption algorithm.

   A. block cipher B. ciphertext

   C. S-AES mode D. Triple DES

2. Triple DES makes use of _________ stages of the DES algorithm, using a total of two or three distinct keys.

   A. nine B. six

   C. twelve D. three

3. Another important mode, XTS-AES, has been standardized by the _________ Security in Storage Working Group.

   A. IEEE B. ISO

   C. NIST D. ITIL

4. The ________ and ________ block cipher modes of operation are used for authentication.

   A. OFB, CTR B. ECB, CBC

   C. CFB, OFB D. CBC, CFB

5. _________ modes of operation have been standardized by NIST for use with symmetric block ciphers such as DES and AES.

   A. Three B. Five

   C. Nine D. Seven

6. The output of the encryption function is fed back to the shift register in Output Feedback mode, whereas in __________ the ciphertext unit is fed back to the shift register.

   A. Cipher Block Chaining mode B. Electronic Codebook mode

   C. Cipher Feedback mode D. Counter mode

7. The simplest form of multiple encryption has _________ encryption stages and _________ keys.

   A. four, two B. two, three

   C. two, two D. three, two

8. The _________ algorithm will work against any block encryption cipher and does not depend on any particular property of DES.

   A. cipher block chaining B. meet-in-the-middle attack

   C. counter mode attack D. ciphertext stealing

9. The _________ method is ideal for a short amount of data and is the appropriate mode to use if you want to transmit a DES or AES key securely.

   A. cipher feedback mode B. counter mode

   C. output feedback mode D. electronic codebook mode

10. _________ mode is similar to Cipher Feedback, except that the input to the encryption algorithm is the preceding DES output.

A. Cipher Feedback B. Counter

C. Output Feedback D. Cipher Block Chaining

11. "Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block", is a description of __________ mode.

A. Cipher Block Chaining B. Counter

C. Cipher Feedback D. Electronic Codebook

12. The _________ mode operates on full blocks of plaintext and ciphertext, as opposed to an *s*-bit subset.

A. CBC B. ECB

C. OFB D. CFB

13. Because of the opportunities for parallel execution in _________ mode, processors that support parallel features, such as aggressive pipelining, multiple instruction dispatch per clock cycle, a large number of registers, and SIMD instructions can be effectively utilized.

A. CBC B. CTR

C. ECB D. CFB

14. _________ mode is suitable for parallel operation. Because there is no chaining, multiple blocks can be encrypted or decrypted simultaneously. Unlike CTR mode, this mode includes a nonce as well as a counter.

A. OFB B. S-AES

C. 3DES D. XTS-AES

15. Both _________ produce output that is independent of both the plaintext and the ciphertext. This makes them natural candidates for stream ciphers that encrypt plaintext by XOR one full block at a time.

A. CBC and ECB B. OFB and CTR

C. ECB and OFB D. CTR and CBC

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

SHORT ANSWER

1. The__________ is a technique in which an encryption algorithm is used multiple times.

2. The most significant characteristic of __________ is that if the same b-bit block of plaintext appears more than once in the message, it always produces the same ciphertext.

3. A __________ 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.

4. Five modes of operation have been standardized by NIST for use with symmetric block ciphers such as DES and AES: electronic codebook mode, cipher block chaining mode, cipher feedback mode, __________, and counter mode.

5. One of the most widely used multiple-encryption scheme is __________ .

6. "The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext" is a description of __________ mode.

7. The simplest mode of operation is the ___________ mode, in which plaintext is handled one block at a time and each block of plaintext is encrypted using the same key.

8. The requirements for encrypting stored data, also referred to as ___________ , differ somewhat from those for transmitted data.

9. The __________ block cipher mode of operation is a general purpose block oriented transmission useful for high speed requirements.

10. "Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext", is a description of the _________ mode of operation.

11. The _________ must be a data block that is unique to each execution of the encryption operation and may be a counter, a timestamp, or a message number.

12. A __________ cipher can operate in real time and eliminates the need to pad a message to be an integral number of blocks.

13. Hardware efficiency, software efficiency, preprocessing, random access, provable security, and simplicity are all advantages of __________ mode.

14. The plaintext of a sector or data unit is organized in to blocks of 128 bits. For encryption and decryption, each block is treated independently. The only exception occurs when the last block has less than 128 bits. In that case the last two blocks are encrypted/decrypted using a ___________ technique instead of padding.

15. The __________ standard describes a method of encryption for data stored in sector-based devices where the threat model includes possible access to stored data by the adversary. Some characteristics of this standard include: the ciphertext is freely available for an attacker, the data layout is not changed on the storage medium and in transit, and the same plaintext is encrypted to different ciphertexts at different locations.