Chapter 2 – Cryptographic Tools

TRUE/FALSE QUESTIONS:

T F 1. Symmetric encryption is used primarily to provide confidentiality.

T F 2. Two of the most important applications of public-key encryption are digital signatures and key management.

T F 3. Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

T F 4. The secret key is input to the encryption algorithm.

T F 5. Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits.

T F 6. Modes of operation are the alternative techniques that have been developed to increase the security of symmetric block encryption for large sequences of data.

T F 7. The advantage of a stream cipher is that you can reuse keys.

T F 8. A message authentication code is a small block of data generated by a secret key and appended to a message.

T F 9. Like the MAC, a hash function also takes a secret key as input.

T F 10. The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

T F 11. Public-key cryptography is asymmetric.

T F 12. Public-key algorithms are based on simple operations on bit patterns.

T F 13. The purpose of the DSS algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

T F 14. An important element in many computer security services and applications is the use of cryptographic algorithms.

T F 15. Some form of protocol is needed for public-key distribution.

MULTIPLE CHOICE QUESTIONS:

1. The original message or data that is fed into the algorithm is __________.

    A. encryption algorithm B. secret key

    C. decryption algorithm D. plaintext

2. The __________ is the encryption algorithm run in reverse.

    A. decryption algorithm B. plaintext

    C. ciphertext D. encryption algorithm

3. __________ is the scrambled message produced as output.

    A. Plaintext B. Ciphertext

    C. Secret key D. Cryptanalysis

4. On average, __________ of all possible keys must be tried in order to achieve success with a brute-force attack.

    A. one-fourth B. half

    C. two-thirds D. three-fourths

5. The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the __________.

    A. SHA B. RSA

    C. AES D. DSS

6. If the only form of attack that could be made on an encryption algorithm is brute-force, then the way to counter such attacks would be to __________ .

    A. use longer keys B. use shorter keys

    C. use more keys D. use less keys

7. __________ is a procedure that allows communicating parties to verify that received or stored messages are authentic.

A. Cryptanalysis B. Decryption

C. Message authentication D. Collision resistance

8. The purpose of a __________ is to produce a "fingerprint" of a file, message, or other block of data.

A. secret key B. digital signature

C. keystream D. hash function

9. __________ is a block cipher in which the plaintext and ciphertext are integers between 0 and *n*-1 for some *n*.

A. DSS B. RSA

C. SHA D. AES

10. A __________ is created by using a secure hash function to generate a hash value for a message and then encrypting the hash code with a private key.

A. digital signature B. keystream

C. one way hash function D. secret key

11. Transmitted data stored locally are referred to as __________ .

A. ciphertext B. DES

C. data at rest D. ECC

12. Digital signatures and key management are the two most important applications of __________ encryption.

A. private-key B. public-key

C. preimage resistant D. advanced

13. A __________ is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

A. mode of operation
B. hash function
C. cryptanalysis
D. brute-force attack

14. Combined one byte at a time with the plaintext stream using the XOR operation, a __________ is the output of the pseudorandom bit generator.

A. keystream
B. digital signature
C. secure hash
D. message authentication code

15. A _________ protects against an attack in which one party generates a message for another party to sign.

A. data authenticator
B. strong hash function
C. weak hash function
D. digital signature

SHORT ANSWER QUESTIONS:

1. Also referred to as single-key encryption, the universal technique for providing confidentiality for transmitted or stored data is __________ .
2. There are two general approaches to attacking a symmetric encryption scheme: cryptanalytic attacks and __________ attacks.
3. The __________ algorithm takes the ciphertext and the secret key and produces the original plaintext.
4. A __________ attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
5. A __________ processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
6. A __________ processes the input elements continuously, producing output one element at a time.
7. Public-key encryption was first publicly proposed by __________ in 1976.

8. The two criteria used to validate that a sequence of numbers is random are independence and _________ .

9. A _________ is a hardware device that sits between servers and storage systems and encrypts all data going from the server to the storage system and decrypts data going in the opposite direction.

10. In July 1998 the __________ announced that it had broken a DES encryption using a special purpose “DES cracker” machine.

11. The simplest approach to multiple block encryption is known as __________ mode, in which plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key.

12. A __________ stream is one that is unpredictable without knowledge of the input key and which has an apparently random character.

13. The __________ is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.

14. __________ is provided by means of a co-processor board embedded in the tape drive and tape library hardware.

15. The purpose of the __________ algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages.

Chapter 2 – Cryptographic Tools

Answer Key

TRUE/FALSE QUESTIONS:

1. T
2. T
3. F
4. T
5. F
6. T
7. F
8. T
9. F
10. T
11. T
12. F
13. F
14. T
15. T

MULTIPLE CHOICE QUESTIONS:

1. D
2. A
3. B
4. B
5. C
6. A
7. C
8. D
9. B
10. A
11. C
12. B
13. D
14. A
15. B

SHORT ANSWER QUESTIONS:

1. symmetric encryption
2. brute-force
3. decryption
4. cryptanalytic
5. block cipher
6. stream cipher
7. Diffie and Hellman
8. uniform distribution
9. back-end appliance
10. Electronic Frontier Foundation (EFF)
11. electronic codebook (ECB)
12. pseudorandom
13. public and private key
14. library-based tape encryption
15. Diffie-Hellman Key Agreement