**Chapter 5: Advanced Encryption Standard**

**TRUE OR FALSE**

T F 1. AES uses a Feistel structure.

T F 2. At each horizontal point, **State** is the same for both encryption and

decryption.

T F 3. DES is a block cipher intended to replace AES for commercial

applications.

T F 4. The nonlinearity of the S-box is due to the use of the multiplicative

inverse.

T F 5. Virtually all encryption algorithms, both conventional and public-

key, involve arithmetic operations on integers.

T F 6. Compared to public-key ciphers such as RSA, the structure of AES

and most symmetric ciphers is quite complex and cannot be

explained as easily as many other cryptographic algorithms.

T F 7. InvSubBytes is the inverse of ShiftRows.

T F 8. The ordering of bytes within a matrix is by column.

T F 9. In the Advanced Encryption Standard the decryption algorithm is

identical to the encryption algorithm.

T F 10. The S-box is designed to be resistant to known cryptanalytic

attacks.

T F 11. As with any block cipher, AES can be used to construct a message

authentication code, and for this, only decryption is used.

T F 12. The inverse add round key transformationis identical to the

forward add round key transformation because the XOR

operation is its own inverse.

T F 13. The Rijndael developers designed the expansion key algorithm to

be resistant to known cryptanalytic attacks.

T F 14. The transformations AddRoundKey and InvMixColumn alter the

sequence of bytes in State.

T F 15. AES can be implemented very efficiently on an 8-bit processor.

**MULTIPLE CHOICE**

1. The Advanced Encryption Standard was published by the \_\_\_\_\_\_\_\_\_\_ in 2001.

A. ARK B. FIPS

C. IEEE D. NIST

2. In Advanced Encryption Standard all operations are performed on \_\_\_\_\_\_\_\_\_\_

bytes.

A. 8-bit B. 16-bit

C. 32-bit D. 4-bit

3. The AES cipher begins and ends with a(n) \_\_\_\_\_\_\_\_\_ stage because any other stage,

applied at the beginning or end, is reversible without knowledge of the key and

would add no security.

A. Substitute bytes B. AddRoundKey

C. MixColumns D. ShiftRows

4. A \_\_\_\_\_\_\_\_\_\_ is a set in which you can do addition, subtraction, multiplication and

division without leaving the set.

A. record B. standard

C. field D. block

5. Division requires that each nonzero element have a(n) \_\_\_\_\_\_\_\_\_\_ inverse.

A. multiplicative B. divisional

C. subtraction D. addition

6. In AES, the arithmetic operations of addition, multiplication and division are

performed over the finite field \_\_\_\_\_\_\_\_\_ .

A. Z*p* B. *a/b = a(b-1)*

C. GF(*2n-1*) D. GF(28)

7. In the AES structure both encryption and decryption ciphers begin with a(n)

\_\_\_\_\_\_\_\_\_\_ stage, followed by nine rounds that each include all four stages,

followed by a tenth round of three stages.

A. Substitute bytes B. AddRoundKey

C. MixColumns D. ShiftRows

8. The final round of both encryption and decryption of the AES structure consists

of \_\_\_\_\_\_\_\_\_\_ stages.

A. one B. two

C. four D. three

9. The first row of State is not altered; for the second row a 1-byte circular left

shift is performed; for the third row a 2-byte circular left shift is performed; and

for the fourth row a 3-byte circular left shift is performed. This transformation

is called \_\_\_\_\_\_\_\_\_\_ .

A. AddRoundKey B. ShiftRows

C. MixColumns D. Substitute bytes

10. In the AddRoundKey transformation the 128 bits of State are bitwise XORed

with the \_\_\_\_\_\_\_\_\_ of the round key.

A. 256 bits B. 128 bits

C. 64 bits D. 512 bits

11. The \_\_\_\_\_\_\_\_\_\_ is when a small change in plaintext or key produces a large change

in the ciphertext.

A. avalanche effect B. Rcon

C. key expansion D. auxiliary exchange

12. The encryption round has the structure:

1. ShiftRows, MixColumns, SubBytes, InvMixColumns
2. SubBytes, ShiftRows, MixColumns, AddRoundKey
3. MixColumns, ShiftRows, SubBytes, AddRoundKey
4. InvShiftRows, InvSubBytes, AddRoundKey, InvMixColumns

13. \_\_\_\_\_\_\_\_\_\_ affects the contents of bytes in State but does not alter byte sequence

and does not depend on byte sequence to perform its transformation.

A. InvSubBytes B. ShiftRows

C. SubBytes D. InvShiftRows

14. In the general structure of the AES encryption process the input to the

encryption and decryption algorithms is a single \_\_\_\_\_\_\_\_\_ block.

A. 32-bit B. 256-bit

C. 128-bit D. 64-bit

15. The cipher consists of *N* rounds, where the number of rounds depends on the

\_\_\_\_\_\_\_\_\_\_ .

A. key length B. output matrix

C. State D. number of columns

**SHORT ANSWER**

1. The \_\_\_\_\_\_\_\_\_\_ is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits.
2. The four separate functions of the Advanced Encryption Standard are: permutation, arithmetic operations over a finite field, XOR with a key, and \_\_\_\_\_\_\_\_\_\_ .
3. The National Institute of Standards and Technology chose the \_\_\_\_\_\_\_\_\_\_ design as the winning candidate for AES.
4. The cipher consists of N rounds, where the number of rounds depends on the \_\_\_\_\_\_\_\_\_\_ .
5. AES processes the entire data block as a single matrix during each round using \_\_\_\_\_\_\_\_\_\_ and permutation.
6. The first N - 1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, AddRoundKey, and \_\_\_\_\_\_\_\_\_\_ .
7. The forward substitute byte transformation, called \_\_\_\_\_\_\_\_\_ , is a simple table lookup.
8. The \_\_\_\_\_\_\_\_\_ transformation operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.
9. The mix column transformation combined with the \_\_\_\_\_\_\_\_\_\_ transformation ensures that after a few rounds all output bits depend on all input bits.
10. The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of \_\_\_\_\_\_\_\_\_\_ words (176 bytes).
11. The standard decryption round has the structure InvShiftRows, InvSubBytes, \_\_\_\_\_\_\_\_\_\_, InvMixColumns.
12. \_\_\_\_\_\_\_\_\_\_\_ affects the sequence of bytes in State but does not alter byte contents and does not depend on byte contents to perform its transformation.
13. A more efficient implementation can be achieved for a 32-bit processor if operations are defined on \_\_\_\_\_\_\_\_\_ words.
14. An example of a finite field is the set Z*p* consisting of all the integers {0, 1, . . . , *p* - 1}, where *p* is a \_\_\_\_\_\_\_\_\_\_ and in which arithmetic is carried out modulo *p*.
15. A polynomial *m(x)* is called \_\_\_\_\_\_\_\_\_\_ if and only if *m(x)* cannot be expressed as a product of two polynomials, both of degree lower than that of *m(x).*