T F 1. DES uses a 56-bit block and a 64-bit key.

T F 2. A problem with the ideal block cipher using a small block size is that it is vulnerable to a statistical analysis of the plaintext.

T F 3. 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.

T F 4. All other things being equal, smaller block sizes mean greater security.

T F 5. Greater complexity in the subkey generation algorithm should lead to greater difficulty of cryptanalysis.

T F 6. Fast software encryption/decryption and ease of analysis are two considerations in the design of a Feistel cipher.

T F 7. A prime concern with DES has been its vulnerability to brute-force attack because of its relatively short key length.

T F 8. 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. "

T F 9. The heart of a Feistel block cipher is the function F, which relies on the use of S-boxes.

T F 10. The strict avalanche criterion and the bit independence criterion appear to weaken the effectiveness of the confusion function.

T F 11. 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. [L SEP]

T F 12. The key schedule algorithm is more popular and has received more attention than S-box design.

T F 13. AES uses a Feistel structure.

T F 14. At each horizontal point, State is the same for both encryption and decryption.

T F 15. DES is a block cipher intended to replace AES for commercial applications.

T F 16. The nonlinearity of the S-box is due to the use of the

multiplicative inverse.

T F 17. InvSubBytes is the inverse of ShiftRows.

T F 18. The ordering of bytes within a matrix is by column.

T F 19. In the Advanced Encryption Standard the decryption algorithm is identical to the encryption algorithm.

T F 20. As with any block cipher, AES can be used to construct a message authentication code, and for this, only decryption is used.

T F 21. The inverse add round key transformation is identical to the forward add round key transformation because the XOR operation is its own inverse.

T F 22. The Rijndael developers designed the expansion key algorithm to be resistant to known cryptanalytic attacks.

T F 23. The transformations AddRoundKey and InvMixColumn alter the sequence of bytes in State.

SHORT ANSWER

1. A _____ 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.

2. _____ 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.

3. Many block ciphers have a _____ 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.

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

5. In _____ 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.

6. Two areas of concern regarding the level of security provided by DES are the nature of the algorithm and the _____ .

7. The _____ 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.

8. The _____ 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.

9. The cryptographic strength of a Feistel cipher derives from three aspects of the design: the function F, the key schedule algorithm, and _____ .

10. Two alternatives to DES are AES and _____ DES.

11. 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.

12. The four separate functions of the Advanced Encryption Standard are: permutation, arithmetic operations over a finite field, XOR with a key, and _____ .

13. The cipher consists of N rounds, where the number of rounds depends on the _____ .

14. AES processes the entire data block as a single matrix during each round using _____ and permutation.

15. The first N - 1 rounds consist of four distinct transformation functions: SubBytes, ShiftRows, AddRoundKey, and _____ .

16. 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.

17. The mix column transformation combined with the _____ transformation ensures that after a few rounds all output bits depend on all input bits.

18. The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of _____ words (176 bytes).

19. The standard decryption round has the structure InvShiftRows, InvSubBytes, _____, InvMixColumns.

20. _____ affects the sequence of bytes in State but does not alter byte contents and does not depend on byte contents to perform its transformation.