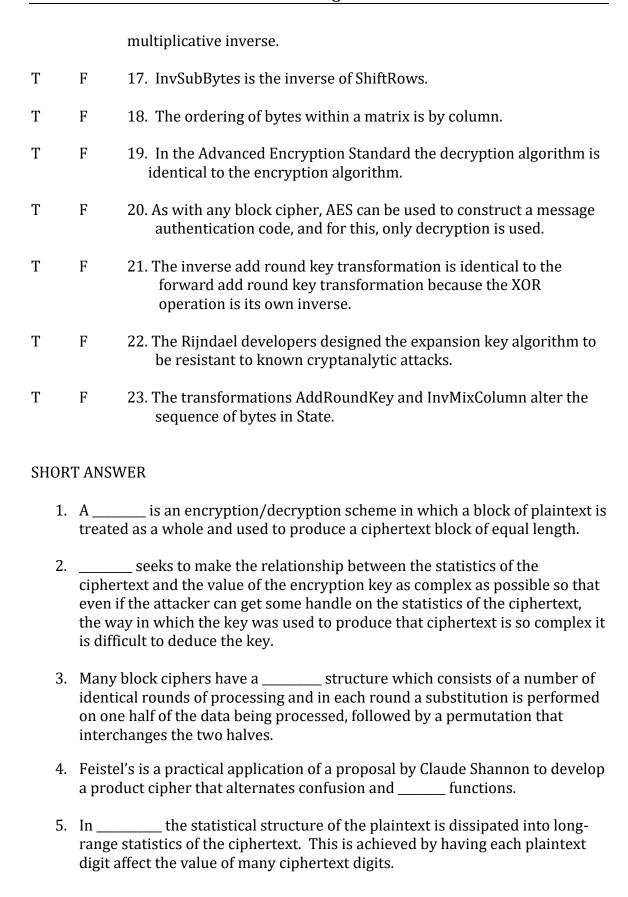
| T | F | 1. DES uses a 56-bit block and a 64-bit key. |
|---|---|--|
| T | F | 2. A problem with the ideal block cipher using a small block size is that it is vulnerable to a statistical analysis of the plaintext. |
| T | F | 3. Confusion seeks to make the statistical relationship between the plaintext 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. |
| Т | 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. " |
| Т | 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. |
| Т | 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. |
| Т | 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 |



| 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 |