1. Also referred to as single-key encryption, the universal technique for providing confidentiality  
for transmitted or stored data is symmetric encryption.  
2. There are two general approaches to attacking a symmetric encryption scheme:  
cryptanalytic attacks and brute-force attacks.  
3. The decryption algorithm takes the ciphertext and the secret key and produces  
the original plaintext.  
4. A cryptanalytic attack exploits the characteristics of the algorithm to attempt to deduce a specific  
plaintext or to deduce the key being used.  
5. A block cipher processes the plaintext input in fixed-size blocks and produces a block of  
ciphertext of equal size for each plaintext block.  
6. A stream cipher processes the input elements continuously, producing output one element at a time.  
7. Public-key encryption was first publicly proposed by Diffie and Hellman in 1976.  
8. The two criteria used to validate that a sequence of numbers is random are independence and  
uniform distribution.  
9. A back-end appliance 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 Electronic Frontier Foundation (EFF) 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 electronic codebook mode, in which  
plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key.  
12. A pseudorandom stream is one that is unpredictable without knowledge of the input key and which  
has an apparently random character.  
13. The public and private key is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.  
14. Library-based tape encryption is provided by means of a co-processor board embedded in the tape drive and tape  
library hardware.  
15. The purpose of the Diffie-Hellman Key Agreement 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.  
**Please choose from the following concepts:**