Name: Nguyễn Việt Hoàng **Student's ID:** B22DCVT214

QUIZ FOR LECTURE 2

A. Determine if each statement is "True" or "False" (5 pts for each correct answer)

1. T F Ciphertext is the scrambled message produced as output.
2. T F The security of symmetric encryption depends on the secrecy of the algorithm, not the secrecy of the key.
3. T F Smaller block sizes mean greater security but reduced encryption/decryption speed.
4. T F The longer the secret key, the faster we can decrypt the ciphertext
5. T F In a symmetric cryptosystem, the sender and receiver must have the same secret key and use the same secret algorithm.
6. T F AES uses a Feistel structure.
7. T F 64-bit key size is used with DES.
8. T F Ideal block cipher requires irreversible mapping so that each ciphertext must be produced by an unique plaintext.
9. T F When using the BF to attack a Ceasar cipher, the more characters we know, the longer time is required to break the code.
10. T F When we increase the number of rounds in the Feistel Cipher, the system becomes more complex but the security is also improved.

B. Select the correct answer for filling the gap (4 pts for each correct answer)

1. _____ is the original message or data that is fed into the algorithm as input.

   A. DES B. Plaintext
   C. Encryption key D. Ciphertext

2. If both sender and receiver use the same key, the system is referred to as _____ encryption.

   A. asymmetric B. two-key
   C. symmetric D. public-key

3. A _____ approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

   A. triple DES B. brute-force
   C. block cipher D. computational

4. The current most common key length in AES is _____ .

   A. 64 bits B. 128 bits
   C. 32 bits D. 200 bits

5. The operation by which rach plaintext element or group of elements is uniquely **replaced by** a corresponding ciphertext element or group of elements is called _____

   A. Permutation B. Substitution
   C. Approximation D. Encryption

C. Complete following sentences by filling the gap (10 pts for each correct answer)

1. Brute-force attack is an approach that tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
2. A system is considered unconditionally secure when no matter how much ciphertext is available, how much time and computing ability an opponent has, it is impossible for attackers to decrypt the ciphertext
3. The simplest and earliest known cipher that was used by Julius Caesar is a kind of substitution cipher.