I. Multiple Choice Questions (5 Marks / Question)

Question 1 – 7

*Choose the best answers from **A**, **B**, **C** and **D**. **ONE** or **MULTIPLE** choice(s) is/are correct.*

*You will get the marks if you select **ALL** correct choice(s) and **NO** wrong choice(s).*

Write your answers in boxes 1 – 7 in your answer book.

1. Which of the following is/are FALSE?

   A. A secure block cipher should be a pseudorandom permutation.
   B. AES has 3 possible values for block size.
   C. In modern cryptography, we should assume that cryptographic algorithms are public.
   D. The result of $(-16)\ mod\ 5$ is -1.

2. Which of the following is/are TRUE?

   A. A passive attacker may break data integrity.
   B. A PDF document can be used as a keystream for Vernam cipher.
   C. Transport Layer Security (TLS) guarantees CIA properties.
   D. The tail of a rainbow table chain is the hash of a password.

3. Which of the following is/are FALSE?

   A. Given a finite field Z_p where p is a prime number, its primitive root g can be used to generate all non-negative integers which are smaller than p.
   B. In TLS, the handshake keys of both Server and Client must be derived from the master secret.
   C. To achieve the same target strength, RSA needs less key length than AES.
   D. In CBC mode, changing IV causes the ciphertexts of all blocks to change.

4. Which of the following is/are TRUE?

   A. Trust is a necessary component in security.
   B. Digital signatures do not protect the confidentiality of the signed data.
   C. The output of a pseudorandom generator (PRNG) is always the same if the seed is the same.
   D. No single security solution can defend all kinds of attacks.

5. Which of the following is/are FALSE?

   A. A 116-bit key can be used in AES according to NIST's recommendation.
   B. PBKDF2 uses HMAC to calculate a key from the password.
   C. Given a message to be encrypted by a key under ECB mode, if two blocks in this message are identical, their ciphertexts are identical.
   D. In Linux, the file `/etc/passwd` stores the hashes of users' passwords.

6. Which of the following are/is TRUE?

A. In self-synchronizing stream ciphers, the keystream is generated from a key and a fixed number of previous plaintext digits.
B. Spoofing attacks are because users cannot be sure who is receiving their passwords.
C. Given a message encrypted under CBC mode, if one block's ciphertext is changed to wrong one after encryption, the decryption of all following blocks is wrong.
D. Given a message of 12 bytes, if we pad it to 16 bytes by CMS, the part to be padded contains 0x04, 0x04, 0x04, 0x04.

7. Which of the following is/are FALSE?

A. To deploy TLS, a server must have a certificate.
B. Given a 48-byte message, the length of its hash under SHA-384 is also 48 bytes.
C. In FIDO2 protocol, the user's browser uses CTAP2 protocol to communicate with the server to log in.
D. Given a dictionary that contains 20 words of 8 letters, if a passphrase based on this dictionary contains 8 words, there are 8^8 possible passphrases.

II. Comprehensive Questions

Question 8 – 15

*You must provide the details in your answers, i.e., the **complete logical reasoning path** about how you get the final results from the given information.*

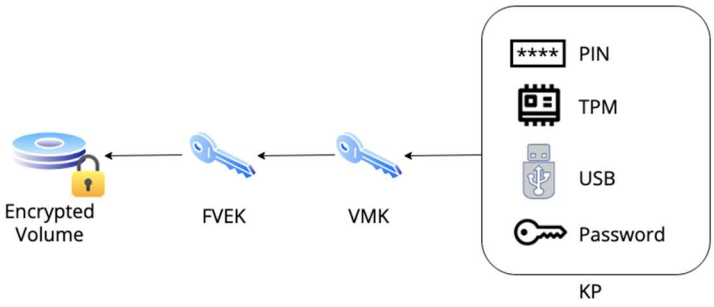
Answers with only final results are not acceptable.

Write your answers in area 8 - 15 in your answer book.

8. (4 marks) Given two blocks b_1, b_2 to be encrypted by the key k and the nonce n under CTR mode, explain why the counters for b_1 and b_2 must be different.

9. (6 marks) Explain why hash functions designed for efficiency are not good for password hashing.

10. (6 marks) Explain why BitLocker does not use VMK to encrypt the data in volume directly.



11. (8 marks) Given an English article is encrypted by Caesar cipher, describe how you can break this encryption by using frequencies of all characters in plaintext language, and explain which feature of Caesar cipher causes this attack.

12. (8 marks) Suppose we have two databases that use different salts to hash their passwords. Database A uses the salt S_A to hash all its passwords, while Database B uses the salt S_B to hash all its passwords. Explain how these two different salts reduce the efficiency of an attacker performing the rainbow table attack.

13. (8 marks) In password guessing, what are the differences between online attack and offline attack? Provide one method against online attack (in one sentence) and one method against offline attack (in one sentence).

14. (10 marks) There is a counter-based stream cipher whose i-th keystream bit is calculated by $ks_i = [(K + CTR_i) \oplus N] \; mod \; 2$ ($+$ is addition, $\oplus$ is XOR, and $mod \; 2$ is to use the last bit), where K is the secret key, CTR_i is the counter, and N is the nonce. If K is 0101 (binary), $N = 1010$ (binary), and CTR starts from 0000 (binary), use this cipher to encrypt data 1101 (binary).

15. (15 marks) The table below shows a cryptographically-secure pseudorandom generator (CSPRNG) for Feistel cipher, where **Data** and **Round Key** are inputs, and **Output** is its output.

Data	**Round Key**	**Output**	**Data**	**Round Key**	**Output**
00	00	01	10	00	00
00	01	01	10	01	00
00	10	10	10	10	10
00	11	11	10	11	00
01	00	00	11	00	01
01	01	10	11	01	01
01	10	11	11	10	11
01	11	11	11	11	10

Given a file to be encrypted 1011 (binary), encrypt it by Feistel cipher in 4 rounds. The round key for each round is 01, 11, 10, 00 (all binaries). Show your calculation details and the final ciphertext.

END