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 TRUE?

   A. In (non-pseudo) Random Permutation, the size of its input is equal to the size of its output.
   B. In AES, the size of key (used to derive round keys) does not need to be equal to the block size.
   C. In a web server, the subject name of its certificate is usually its domain name.
   D. HTTPS is HTTP protocol protected by TLS.

2. Which of the following is/are FALSE?

   A. NIST does not require to force the use of special symbols in password currently.
   B. Cryptoanalysis is about how to attack a cryptosystem.
   C. A truly random number is generated by an algorithm through a seed.
   D. To encrypt one message, in each step, a stream cipher generates one binary keystream bit for encryption.

3. Which of the following is/are TRUE?

   A. It is a good choice to use $h(p)$ to hash a password p, where $h(x)$ is a SHA-2 function.
   B. In system design, a security measure introduces additional costs.
   C. A hash function SHA-384 is based on Merkle-Damgård construction.
   D. A hash function does not provide confidentiality.

4. Which of the following is/are FALSE?

   A. Diffie-Hellman cannot be used for signing signature.
   B. A self-signed certificate cannot inherit trust from other certificates.
   C. If a user uses FIDO2 to log in to a system, it does not provide a password to server.
   D. In Authenticated Encryption, MAC-then-Encrypt is better than Encrypt-then-MAC.

5. Which of the following is/are FALSE?

   A. If a 4-unit password has 4 possibilities for each unit, we need an at least 8-bit binary number to represent it.
   B. To calculate hashes efficiently, it prefers to use GPUs instead of CPUs.
   C. In Rainbow Tables, given a hash, a reduction function is to find a password whose hash is equal to the input hash.
   D. Given a message of 14 bytes, its AES ciphertext is of 14 bytes.

6. Which of the following are/is TRUE?

A. To protect a message by CBC, IV in decryption must be equal to IV in encryption.
B. None of the modes of operations in AES provide integrity.
C. In Bitlocker, Volume Master Key is protected by Full Volume Encryption Key.
D. X25519 curve defines a specific p and g for Diffie-Hellman.

7. Which of the following is/are FALSE?

A. In hash functions, weak collision resistance suffers from the birthday paradox.
B. In Authenticated Encryption with Associated Data, the associated data is not encrypted.
C. In Stream Cipher, the length of keystream to be used must be equal to the length of plaintext to be encrypted.
D. In CBC mode, a plaintext block to be encrypted should be XORed by the last plaintext block before being processed by a block cipher.

II. Comprehensive Questions

Question 8 – 15

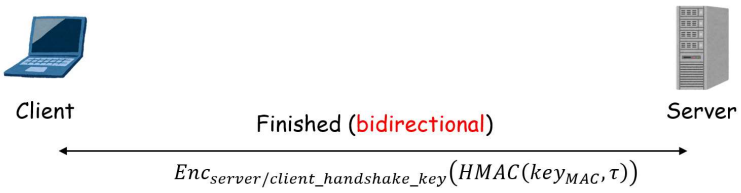
*You must provide the details in your answers, i.e., the **complete logical reasoning path** about how you get the final results from the given information.*

Answers with only final results are not acceptable.

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

8. (6 marks) Describe how a server verifies an HOTP from a user and why it can ensure that the user who passes the verification must be the legitimate user.

9. (4 marks) At the end of TLS handshake protocol, why do Client and Server calculate the HMAC of transcript and exchange it to make sure it is equal?



10. (6 marks) In RSA, why does the decryption fail if the plaintext m is larger than or equal to $n = pq$, where p and q are prime numbers? Explain the reasons.

11. (8 marks) Given a document m, its signature σ generated by a public key pk, a secret key sk and a hash function $H(x)$, if σ cannot pass the verification (suppose that the verifier uses the correct signature algorithm and the same hash function), **explain two main reasons and discuss why these reasons can lead to verification failures**. (You may define any other notations if you need them, but please provide their definitions.)

12. (6 marks) If a hash function $H(x)$ does not meet the weak collision resistance, describe how it cannot ensure the integrity.

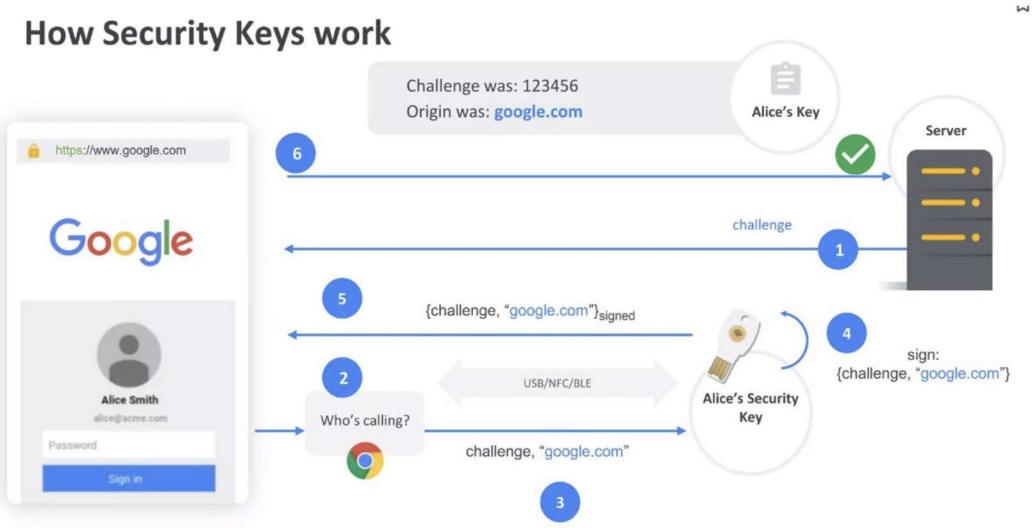
13. (12 marks) We have a function $f: \{0,1\}^4 \rightarrow \{0,1\}^4$ that takes a 4-bit binary number as input and generates a 4-bit binary number as output. The map from inputs to outputs is listed as follows.

Input	Output	Input	Output
0000	0001	1000	0111
0001	0100	1001	1010

0010	0101	1010	0000
0011	0010	1011	1000
0100	1001	1100	1111
0101	1101	1101	1011
0110	1110	1110	1100
0111	0011	1111	0110

Given a message 011010 (binary), use **sponge construction** to generate its hash by f.
The block size is set as **2 bits**, and the length of hash result is set as **4 bits**. Please provide the calculation details.

14. (8 marks) In FIDO2 protocol, if a server sends out the **same** challenge number in every login attempt, design an attack that allows an attacker who does not know Alice's secret key to log in to the system as Alice. You should describe what an attacker does step by step and explain why this attack works.



15. (15 marks) Suppose we have a block cipher whose inputs and outputs are listed as follows. The block size is **4 bits**. (Please note that this table is **NOT** identical to the table in Question 13.)

Input	**Output**	**Input**	**Output**
0000	0111	1000	0011
0001	1110	1001	0000
0010	1000	1010	0100
0011	0110	1011	0001
0100	1100	1100	0101
0101	1111	1101	1101
0110	1011	1110	1001
0111	1010	1111	0010

Please note that the key K to be used has **already embedded** in the block cipher. You do not need to consider the key. The table is corresponding to $Enc_K(Input) = Output$.
Given a message 011011001101 (binary), use CTR mode to encrypt this message. The nonce is set as 10 (binary) and the counter starts from 00 (binary). Please provide the calculation details.

END