1. (1 pt) The ciphertext character frequency shown in the attached figure most likely corresponds to the following cipher

A. Caesar cipher
B. transposition cipher
C. shift cipher with the key $k=2$
D. affine cipher with the key $(k_1, k_2)$, where $k_1=1$ and $k_2=24$
E. Vigenere cipher with the period $d=2$, and the $K=(2, 24)$
F. Playfair cipher
G. ENIGMA

![Standard English character frequency](image1.png)

![Ciphertext character frequency](image2.png)
2. (1 pt) Arrange the following ciphers in the order of the increasing security. Assume that an attacker has access to a ciphertext obtained by encrypting 1000-letter message with a given cipher (start from the cipher which is the easiest to break).

A. running key cipher
B. affine cipher
C. Ceaser cipher
D. general monoalphabetic cipher
E. shift cipher
F. Enigma
G. Vigenère cipher with the period d=5
H. general polyalphabetic cipher with the period d=3
I. letter-based Vernam cipher with the encryption described by the equation
   \[ c_i = m_i + k_i \mod 26 \], where \( m_i \) is a code of the plaintext letter, \( c_i \) is a code of the ciphertext letter, and \( k_i \) is a code of the keystream letter; the keystream is generated at random and can be used only once.

3. (1 pt) In the ciphertext obtained using the Vigenère cipher, a four-character sequence XACT appears at positions 256, 436, and 856. Additionally, the measure of roughness for this ciphertext is equal to 0.0028. Based on this information, the most likely period of the Vigenère cipher is:
   A. 1
   B. 2
   C. 3
   D. 4
   F. 6
   G. 12
   H. 60

4. (1 pt) Select all attack types that can be efficiently used to break the Vigenère cipher with \( d > 10 \) (the number of correct answers may be greater than one)
   A. Kasiiski’s method
   B. linear cryptanalysis
   C. frequency analysis of single ciphertext characters
   D. method of index of coincidence
   E. frequency analysis of ciphertext digrams
   F. exhaustive key search
   G. differential cryptanalysis
5. (1 pt) The major **advantages** of the inverse CBC mode of DES, for which encryption transformation is given below are (**more than one answer may be correct**):

A. decryption can be parallelized  
B. encryption can be parallelized  
C. preprocessing can be used for decryption  
D. the same plaintext block is always encrypted to the same ciphertext block  
E. the mode is suitable for a fast random read access to the block $m_j$  
F. the mode is suitable for a fast random write access to the block $m_j$  
G. mounting exhaustive key search typically requires guessing two consecutive blocks of the message  
H. decryption circuit does not introduce any overhead on top of the encryption circuit, independently of the type of the block cipher used.

6. (1 pt) Which of the following five security services are implemented by the protocol given below?

1. A sends to B
   
   A, $E(PU_B, (M \| A) \| E(PR_A, h(M \| A)))$, B

2. B sends to A
   
   B, $E(PU_A, (M \| B))$, A

X represents a unique name of user X, where X=A or B  
M means a message  
$(M \| X)$ means M concatenated with X  
$E(PU_Y, Z)$ means Z encrypted using a public key of Y  
$E(PR_Y, Z)$ means Z encrypted using a private key of Y  
h(M) means a hash value of M.

A. Confidentiality  
B. Authentication of the Sender  
C. Authentication of the Receiver  
D. Non-repudiation of the Sender  
E. Non-repudiation of the Receiver
Short problems

1. (3.5 pt) Using only two types of rectangular boxes (D and C), representing respectively
   
   • secret-key block cipher decryption D, with a 64-bit input, 64-bit output, and a 128-bit key K
   
   • lossless data compression C, with an arbitrary input size, and the corresponding output size,

   and a condition box, draw a graphical diagram showing how these operations can be used to implement simultaneously the following two security services:

   a. confidentiality, and
   
   b. authentication

   for the message M, composed of N message blocks denoted by \( m_1, m_2, m_3, \ldots, m_N \).

   Please clearly specify in which order you recommend performing transformations responsible for compression, confidentiality, and authentication, respectively.

   Explain the reasons for this specific order.

   Assume that you cannot use the corresponding encryption E or any other cryptographic operation, such as hash function, or public key encryption/decryption.

2. (3.5 pts) Solve the following system of two equations with two unknowns, \( x \) and \( y \), in the arithmetic modulo 39, i.e., find ALL possible values of pairs \((x, y)\), for which both equations hold.
   
   \[
   26 \cdot x + y \equiv 24 \pmod{39} \\
   2 \cdot x + y \equiv 9 \pmod{39}
   
   \]

3. (3.5 pts) Encrypt the message "A FRIEND IN NEED IS A FRIEND INDEED" using the Vigenère cipher with the key "CARE".

   Compute the index of coincidence of the obtained ciphertext (you do not have to reduce it to a single number, but you need to replace variables in the I.C. equation with actual numbers).

   Can the period of this cipher be determined using the Kasiski’s method based on the obtained ciphertext? If so, how? If not, why?
4. (3.5 pts) Compute the bits number 16, 32, 48, and 64 at the output of the first round of the DESX encryption, assuming that the plaintext block is equal to \(M=\text{"C000 0000 0000 0000"}\), the key \(K_a\) is equal to \(\text{"0000 0000 0000 0003"}\), and the round key \(K_1\) computed based on the 56-bit key \(K\) is equal to \(\text{"ABCD EF01 2345"}\) (all values in the hexadecimal notation).

5. (3.5 pts) Suppose the DES Mangler function \(F\) mapped every 32-bit input \(R\), regardless of the value of the 48-bit input \(K\), to
   a) 32-bit string of zeros,
   b) the value of \(R\).
   What would be the expression for \(R_{16}\) and \(L_{16}\) as a function of \(L_0\) and \(R_0\) during encryption?
   What would be the expression for \(L_0\) and \(R_0\) as a function of \(R_{16}\) and \(L_{16}\) during decryption?
   Derive all equations separately for the case a) and for the case b).
   Hint:
   You can use the following properties of the xor operation:
   
   \((A \text{ xor } B) \text{ xor } C = A \text{ xor } (B \text{ xor } C)\)
   
   \(A \text{ xor } A = 0\)
   
   \(A \text{ xor } 0 = A\)
   
   \(A \text{ xor } 1 = \text{ bitwise complement of } A\)

   where

   \(A, B, C\) are \(n\)-bit strings of bits
   
   \(0\) is an \(n\)-bit string of zeros
   
   \(1\) is an \(n\)-bit string of ones.