Q1. (3 pts) Which of the following five security services are implemented by the protocol given below? For any security services that are not implemented, explain why they are not implemented.

1. A sends to B
   \[ A, \ E(\text{PU}_B, \ M \ || \ h(\text{M} \ || \ A)), \ B \]

2. B sends to A
   \[ B, \ E(\text{PR}_B, \ M \ || \ h(\text{M} \ || \ B)), \ A \]

Notation:
- X represents a unique name of user X, where X=A or B
- M means a message (the same in both transfers)
- (M \ || \ X) means M concatenated with X
- E(\text{PU}_Y, Z) means Z encrypted using a public key of Y
- E(\text{PR}_Y, Z) means Z encrypted using a private key of Y
- h(M) means a hash value of M.

1. Confidentiality
2. Authentication of the Sender
3. Authentication of the Receiver
4. Non-repudiation of the Sender
5. Non-repudiation of the Receiver

Q2. (1 pt) Draw a diagram illustrating the internal operation of a MAC (Message Authentication Code) generation function based on a hash function, h, only.

Q3. (1 pts) Give at least two reasons why compression should be executed before secret key encryption when implementing confidentiality.

Q4. (1 pt) Calculate an output from the Radix 64 conversion of the following sequence of 3 bytes expressed in the hexadecimal notation: “89ABCD”.

Q5. (1 pt) Explain the role of the field “Owner Trust” in the PGP Public Key Ring. What are the valid values of this field, and how they are used?

Q6. (1 pt) Select all attack types that can be efficiently used to break the general polyalphabetic cipher with unknown \( d > 2 \) (the number of correct answers may be greater than one)

A. Kasiski’s method
B. frequency analysis of diagrams
C. method of index of coincidence
D. exhaustive key search
E. none of the above
Part 2

Q7. (3 pts) Break the affine cipher (i.e., find the key $K=(k_1, k_2)$) based on the knowledge that

- the most frequent letter of the ciphertext is 'P'
- the second most frequent letter of the ciphertext is 'U'
- the most frequent trigram is ‘ZSH’.

Q8. (3 pts) Compute the bits number 8, 16, 40, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is equal to $C=$"9000 0000 0000 0009”, and the round key $K_{16}$ is equal to “CCCC DDDD EEEE” (all values in the hexadecimal notation).

Q9. (3 pts) Suppose the DES Mangler function $F$ mapped every 32-bit input $R$, regardless of the value of the 48-bit input $K$, to $f(R, K) = R \oplus K$, where $K$ is a constant, equal to FFFF0000 in the hexadecimal notation.

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?

Q10. (3 pts) Encrypt the message $M =$ “A GOOD BEGINNING MAKES A GOOD ENDING” using Playfair cipher with the key $K =$ “PROCRASTINATION IS THE THIEF OF TIME”.

Use Stalling’s convention for the Playfair cipher.