Q1. (3 pts)

Implemented services:
- Authentication of the Receiver
- Non-repudiation of the Receiver
(1 pt).

Not implemented services:
- Confidentiality – because the ciphertext sent by B to A can be decrypted using the public key of B, available to all users of the network (1 pt).
- Authentication of the sender – because everybody with access to the public key of B could execute step 1 of the protocol (0.5 pt).
- Non-repudiation of the sender – because everybody with access to the public key of B could execute step 1 of the protocol (0.5 pt).

Q2. (1 pt)

\[ \text{MAC}_K(M) = h(K || M) \]

Q3. (1 pt)

- An encrypted message (ciphertext) is a random string of bits, which does not contain any redundancy. As a result, an output from encryption cannot be compressed any longer, which affects the transmission time.
- By removing redundancy from an input to encryption, the compression makes cryptanalysis more difficult.
Q4. (1 pt)

“89ABCD” = “100010011010101111001101”

By dividing this string into 6-bit blocks, and performing conversion, we obtain:

100010\textsubscript{2} = 34 \rightarrow i
011010\textsubscript{2} = 26 \rightarrow a
101111\textsubscript{2} = 47 \rightarrow v
001101\textsubscript{2} = 13 \rightarrow N

\textbf{Answer:} iavN

Q5. (1 pt)

The “Owner Trust” field is used to indicate the degree to which an owner of a public key ring trusts the owner of a given public key to introduce other users to him/her, and sign their public keys.

The allowed values are:
- undefined trust
- unknown user
- usually not trusted to sign other keys
- usually trusted to sign other keys
- always trusted to sign other keys
- this key is present in private key ring (ultimate trust).

When a new public key is imported to the public key ring, one or more signatures may be attached to it. The program locates owners of public keys who generated these signatures, and then copy their “Owner Trust” field to the “Signature Trust” field of the given signatures. Afterwards, the value of the “Key Legitimacy” field is calculated for the new entered public key. This value is calculated by PGP as a weighted sum of the “Signature Trust” fields, where a weight of 1/X is given to signatures that are always trusted and 1/Y to the signatures that are usually trusted. X and Y are user-configurable parameters, e.g., X=1 and Y=2. When the total sum of weights exceeds 1, the Key Legitimacy is set to “Complete Trust”.

Q6. (1 pt)

A. Kasiski’s method
C. Method of index of coincidence.