Q1 RSA algorithm is under consideration. Assume that $p = 7$ and $q = 11$, determine
(a) [5 pnts] $e$ as the smallest value can be selected;
(b) [5 pnts] calculate $d$;
(c) [5 pnts] providing $M = 26$ calculate $C$.

Answer
(a) $n = pq = 77$, $\varphi(n) = 60$, $\gcd(e, 60) = 1 \Rightarrow e = 7$.
(b) $ed = 1 \mod \varphi(n) \Rightarrow$ if $k = 5$ then $d = 43$.
(c) $26^7 \mod 77 = 5$.

Q2 [10 pnts] Carefully describe the difference between encryption and authentication with regards to modern asymmetric cryptography.

Answer
Main difference between encryption and authentication regarding public cryptography is in the order the two keys are used. When sender prepares a message to a recipient he can use either his private key or recipient’s public key. In the first case he authenticates message while in the second case he prepares confidential message.

If A prepares a message to B and encrypts it using A’s private key before transmitting it. B can decrypt the message using A’s public key. Because the message was encrypted using A’s private key, only A could have prepared the message. Therefore, the entire encrypted message serves as a digital signature. In addition, it is impossible to alter the message without access to A’s private key, so the message is authenticated both in terms of source and data integrity. In contrary, if A prepares a message to B and encrypts it using B’s public key then the message can be decrypted using B’s private key only. This is the way how encryption/decryption in terms of confidential communication between sender and recipient is established and done. In addition, it is possible to authenticate and encrypt a message. This is done by using both sender’s private and recipient’s public keys. When decrypting recipient uses sender’s public key and his own private key.
Q3 [5 pts] Given \( n = 143 \) find \( \varphi(n) \).

Answer
If \( n = 143 \) then \( p=11, q=13 \) or vice versa. In both cases, \( \varphi(n) = (p-1)(q-1) = 10 \times 12 = 120. \)

Q4 [2 pts each] Decide whether each of the following statements is either true or false. Circle the right answer.

- T F (a) RSA is more secure compared to symmetric ciphers.
- T F (b) It is computationally easy to determine the decryption key given knowledge of the cryptographic algorithm and the encryption key.
- T F (c) Either of the related keys can be used for encryption, with the other used for decryption.
- T F (d) It is computationally easy for party A to generate a pair of keys \( K_{U_b} \) and \( K_{R_b} \).
- T F (e) It is computationally infeasible for an opponent, knowing the public key \( K_{U_b} \) and a ciphertext, \( C \), to recover the original message, \( M \).