1. For RSA with the choice of $p=13$ and $q=17$.
   a) Explain why we cannot choose 3 as the public exponent. (2 point)
   b) What is the private exponent if we choose the public exponent as $e=5$ (3 points)
   c) For $e=5$, what is the encryption of 12? Verify decryption (6 points)

2. Explain the following statement: “If all redundancies are removed before encrypting a message, we can avoid brute-force attacks”. Nevertheless, we deliberately add some redundancies (which make brute-force attacks feasible). Why? (5 points)

3. Briefly describe the following types of attacks ($3 \times 4 = 12$ points)
   a) Reflection
   b) Man in the Middle
   c) Replay
   d) Meet-in-the-Middle

4. To send a signed, encrypted and compressed message, what is the typical sequence in which encryption, compression and signing are performed? Why? (4 points)

5. What is the purpose of the “authenticator” in Kerberos? (3 points)

6. Explain the need for forward and reverse signatures in PKI. (5 points)

7. Multiple Kerberi is used when two organizations desire to share a server. How is this achieved? Can you explain the rationale for sharing a secret between the TGSs of the organization (instead of the authentication server)? (4 points)

8. Explain the following terms in the context of PGP ($3 \times 2 = 6$ points)
   a) Key legitimacy
   b) Owner Trust
   c) Signature Trust