Exercise No. 01: *(Mathematical concepts)*

- Apply Fermat's test on p=11, with a=2 and a=3.
- Calculate Φ (19), Φ (21), Φ (8)
- Calculate 513 mod 71 using the fast exponentiation algorithm.

Exercise No. 2: *(RSA encryption)*

Let p = 7 and q = 19

1. Describe the key generation scheme, encryption scheme, and decryption scheme.
2. Prove that DKpv(EKpb(m)) = m.
3. Calculate N and Φ (n).
4. We propose e = 5. Calculate the private key d.
5. Encrypt the plaintext m = 6.
6. Decrypt the ciphertext c= 62.

Exercise No. 3: (Diffie-Hellman Protocol)

1. What is the purpose of the Diffie-Hellman protocol?
2. Determine the Diffie-Hellman session key if Alice communicates the numbers g = 3 and p = 23 to Bob, given that Alice selects the random number a = 5 and Bob selects the number b = 7.
3. Explain the weaknesses of the Diffie-Hellman protocol.
4. Propose a MITM type attack scenario.

Exercise No. 4: (Hash Functions)

1. What properties must hash functions check?
2. Give examples of applications of hash functions.
3. What is the difference between MDC and HMAC type functions?
4. Which of these hash functions are secure: MD-5, SHA-3, SHA-1, SHA-512?
5. Why is a hash function a better way to verify integrity than a checksum such as the Internet checksum?