# Basics of Cryptography for Blockchain – EXERCISES

**Exercise 1**

TRUE or FALSE?

1.1) A Bitcoin address is usually represented using Base16check (False)

1.2) ASCII can be used to encode only characters that can be printed (False)

1.3) The output of a cryptographic hash function has always the same size (i.e., number of bits), no matter the size of the input (True)

1.4) When using the cryptographic hash function MD5, it is impossible that two input messages map to the same hash (False)

1.5) Given an integer number, the number of digits required to represent it using Base-16 is always lower than (or equal to) the number of digits required to represent it using Base-2 (True)

1.6) Can 0xabb67ad99 be the Base16 representation of a 40-bit sequence? (False)

**Exercise 2**

Given the Base16 number 0x86d, answer the following questions:

2.1) What number is it in Base10?

8 \* (16^2) + 6 \* (16^1) + 13 \* (16^0) = 8 \* 256 + 96 + 15 = 2157

2.2) Is 1000 0110 1101 its correct representation in Base2?   
Demonstrate your claim (that is, show the conversion process explicitly)  
  
1 \* (2^11) + 0 \* (2^10) + 0 \* (2^9) + 0 \* (2^8) + 0 \* (2^7) + 1 \* (2^6) + 1 \* (2^5) + 0 \* (2^4) + 1 \* (2^3) + 1 \* (2^2) + 0 \* (2^1) + 1 \* (2^0) = 2157

**Exercise 3**

Convert the Base10 number 678 in Base16 and Base2   
(show the conversion process explicitly)

A piece of paper with writing on it

Description automatically generated

**Exercise 4**

True or False?

1.1) In public encryption, the private key is used for encrypting messages (False)

1.2) A digital signature is the hash of a message m encrypted using the signer (sender) public key (False)

1.3) A digital signature is the hash of a message m encrypted using the signer (sender) private key (True)

1.4) Digitally signed messages are always encrypted (False)

**Exercise 5**

2.1) Consider the Caesar cypher and a meaningful message m in English that has been encrypted using it; the obtained cyphertext c is “isvjrjohpu pz mhuahzapj”.   
Which key (n) was used? What is the message?  
[consider only small letters in the 26-letter English alphabet]

Key: 19

Message: blockchain is fantastic

2.2) Consider the OTP cypher. Given the key 1111 0101 0110 0000, what is message m that generates the cyphertext 0101 0101 0101 1110?

1010 0000 0011 1110

2.3) Consider a special version of the OTP cypher that works using 4-character long string encoded using ASCII encoding.   
Given the key k = (ACK TAB TAB DEL) constituted only of non-printable characters, what is the cypher c of the message m = (J a c k)

Binary representation of the key k (1), m (1) and the cypher c (3):

1. 0000 0110 0000 1001 0000 1001 0111 1111
2. 0100 1010 0110 0001 0110 0011 0110 1011
3. 0100 1100 0110 1000 0110 1010 0001 0100 (Answer)

The cyphertext: L h j DC4 (where DC4 is a control character)

**Exercise 6**

In an RSA encryption system, let p=11 and q=13 and e=7.

3.1) Demonstrate that d=103 is a correct choice

* (e \* d) / ((p-1) \* (q-1)) = (7 \* 103) / (10 \* 12) = 721 / 120 = 6 \* 1 20 + 1 (remainder)

3.2) Encrypt the message m=5

* public key: (11\*13, 7) -> (143, 7)
* private key: (143, 103)
* c (cyphertext) = m^7 mod 143 = 5^7 mod 143 = 47

3.3) Decrypt the message c= 97

- decrypted message = c^d mod n = 97^103 mod 143 = 124