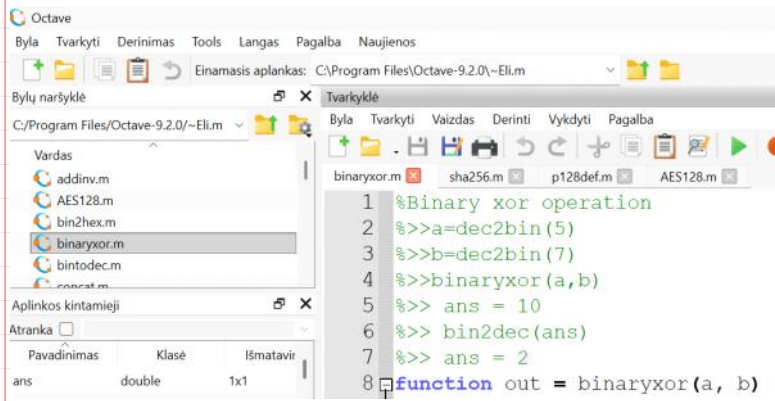




$$\begin{array}{r}
 m: \quad 1001 \ 1011 \ 0110 \\
 k: \oplus \quad 0101 \ 1001 \ 0011 \\
 \hline
 c: \quad 1100 \ 0010 \ 0101 \\
 k: \oplus \quad 0101 \ 1001 \ 0011 \\
 \hline
 m: \quad 1001 \ 1011 \ 0110
 \end{array}$$

%Binary xor operation

% >> a=dec2bin(5)

a = 101

% >> b=dec2bin(7)

b = 111

% >> binaryxor(a,b)

% >> ans = 10

% >> bin2dec(ans)

% >> ans = 2

Binary	Dec	Hex
0000	0	0 _h
0001	1	1 _h
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F _h

% Encryption

>> AEN = int64(123456789) % arbitrary encrypted number

AEN = 123456789

>> AENb=dec2bin(AEN)

AENb = 111010110111100110100010101

>> k = randi(2^28-1)

k = 2.1127e+08

>> k = int64(randi(2^28-1)) % encryption key generated at random

k = 153880907

>> kb = dec2bin(k)

kb = 1001001011000000100101001011

>> cb = binaryxor(AENb,kb) % ciphertext computed by bitwise XOR'ing

cb = 1110011101111100010001011110

>> c=bin2dec(cb)

c = 2.4273e+08

>> c=int64(bin2dec(cb))

c = 242730078

% Decryption

>> mmb=binaryxor(cb,kb)

mmb =

111010110111100110100010101

>> mm=bin2dec(mmb)

mm = 1.2346e+08

>> mm=int64(bin2dec(mmb))

mm = 123456789

% AES128(in,kh32,NR,fun) Advanced Encryption Standard symmetric cipher with key length of 128 bits

% Encryption is performed for 1 block of length 128 bits or 16 ASCII symbols

%

% in - plaintext/ciphertext of string type: maximum 16 symbols or shorter

```

%
% kh32 - shared secret key in hexadecimal number of length=32 (128 bits)
% kh32 can be obtained when shared decimal key k is given using commands:
%   >> k=int64(randi(2^28))
%   k = 160966896
%   >> kh32=dec2hex(k,32)
%   kh32 = 0000000000000000000000000099828F0
%
% NR - Number of Rounds (e.g. Nr = 10)
%   The smaller NR, the lower security of encryption but the speed of encryption is higher
%   The least number of NR is 1 and in this case security lack is evident
%
% fun - letter determining either encryption: fun='e' or decryption: fun='d' functions
%
% Encryption example:
% >> in = 'Hello Bob';
% >> kh32 = '0000000000000000000000000099828F0';
% >> NR = 10;
% >> Ch = AES128(in,kh32,NR,'e')
% ASCII_e = ?1 ~mV % ciphertext in ASCII format
% Ch = 0f9a2c08d191310fb27ed16d90f45686 % ciphertext in hexadecimal format
%
% Decryption example:
% >> Dh = AES128(Ch,kh32,NR,'d')
% Dh = 00000000000048656c6c6f7720426f62 % decrypted message in hex format
% D = Hello Bob % Decrypted message in ASCII format
%

```