```
>> p=int64(genstrongprime(28))
>> p= int64(268435019)
p = 268435019
>> g=2
g = 2

>> x =int64(randi(p-1))
x = 927980
>> a=mod_exp(g,x,p)
a = 86875643
```

```
>> M='Hello Bob'
M = Hello Bob
>> h=hd28(M)
h = 198770750

>> i =int64(randi(p-1))
i = 233191723
>> i_m1=mulinv(i, p-1)
i_m1 = 42019497
>> mod(i*i_m1,p-1)
```

```
>> r=mod_exp(g,i,p)
r = 238149225
>> hmxr=mod(h-x*r,p-1)
hmxr = 199444326
>> s=mod(hmxr*i_m1,p-1)
s = 137708428
```

```
>> V1=mod_exp(g,h,p)
V1 = 16540280
>> a_r=mod_exp(a,r,p)
a_r = 254606533
>> r_s=mod_exp(r,s,p)
r_s = 60867189
>> V2=mod(a_r*r_s,p)
V2 = 16540280
```

```
>> m=111222
m = 111222

>> i =int64(randi(p-1))
i = 135680927
>> a_i=mod_exp(a,i,p)
a_i = 88176259
>> E=mod(m*a_i,p)
E = 134894352
>> D=mod_exp(g,i,p)
D = 137490703
```

```
>> D_mx=mod_exp(D,p-1-x,p)
D_mx = 40036465
>> D_x=mod_exp(D,x,p)
D_x = 88176259
>> mod(D_x*D_mx,p)
ans = 1

>> mm=mod(E*D_mx,p)
mm = 111222
```

```
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 = 00000000000000000000000099828F0
%
% 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 encription: fun='e' or decryption: fun='d' functions
```

```
>> in='111222'
in = 111222

>>  k = int64(160966896)
k = 160966896
```

```
>> in=c
in = 24574b2424572e622498ef6249cfc736

>> fun='d'
fun = d
```

```
>>  k = int64(160966896)
k = 160966896
>> kh32=dec2hex(k,32)
kh32 = 00000000000000000000000000099828F0
>> NR=1
NR = 1
>> fun='e'
fun = e
>> in='111222'
in = 111222
>> c=AES128(in,kh32,NR,fun)
new = $WK$$W.b$bI6
c = 24574b2424572e622498ef6249cfc736
```

```
>> fun='d'
fun = d
>> mmm=AES128(in,kh32,NR,fun)
Out = 00000000000000000000313131323232
mmm = 111222
```