

```
>> p=genstrongprime(28)
```

```
p = 160846019
```

```
>> isprime(p)
```

```
ans = 1
```

```
>> q=(p-1)/2
```

```
q = 80423009
```

```
>> isprime(q)
```

```
ans = 1
```

```
p=268435019;
```

```
>> g=2
```

```
g = 2
```

```
>> mod_exp(g,q,p)
```

```
ans = 160846018
```

```
>> mod_exp(g,2,p)
```

```
ans = 4
```

```
p=268435019; g=2.
```

A:

```
>> u=randi(p-1)
```

```
u = 244318599
```

```
>> A=mod_exp(g,u,p)
```

```
A = 9071422
```

```
>> kAB=mod_exp(B,u,p)
```

```
kAB = 106283239
```

B:

```
>> v=randi(p-1)
```

```
v = 120705651
```

```
>> B=mod_exp(g,v,p)
```

```
B = 189577416
```

```
>> kBA=mod_exp(A,v,p)
```

```
kBA = 106283239
```



Vernam Cipher

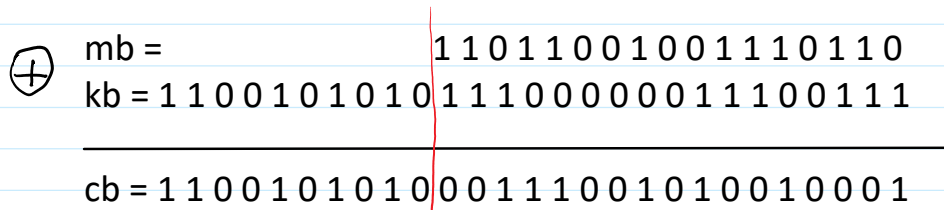
```
>> m=111222
```

```
>> mb=dec2bin(m)
```

```
mb = 11011001001110110
```

```
>> kb=dec2bin(k)
```

```
kb = 110010101011100000011100111
```



```
c = 106197649
```

ElGamal Encryption

B: $PrK_A = \alpha$

```
>> m
```

```
m = 111222
```

```
>> r=randi(p-1)
```

```
r = 145788355
```

```
>> a = r * mod_exp(g, r, p)
```

$c = (E, D)$

A: $PrK_A = x$; $Pub_A = \alpha$.

```
>> D_mx=mod_exp(D,p-1-x,p)
```

```
D_mx = 76735184
```

```
>> r=randi(p-1)
r = 145788355
>> a_r=mod_exp(a,r,p)
a_r = 64567246
>> E=mod(m*a_r,p)
E = 124606324
>> D=mod_exp(g,r,p)
D = 143485917
```

```
>> D_mx=mod_exp(D,p-1-x,p)
D_mx = 76735184
>> mm=mod(E*D_mx,p)
mm = 111222
```