EL_Gamal_And_Diffie_Hellma

```
# Choose a prime and test that it is prime
# Alice does this
p = 71
is_prime(71)
a = mod(2,p)  # primitive root modulo p
```

```
A = 40;# this is the private key
B = a^A; B # this is the public key
```

```
32
```

```
m = 62; # message
k = 30; # random integer <p
Message_key = B^k
C = [a^k,Message_key*m]; C # this outputs c1 and c2 to be sent to Bob
```

```
[20, 14]
```

```
# BOb then proceed this way
C[1]/C[0]^A # since aonly alice knows the key A, only Alice can decrypt the message
```

```
62
```

Use Large prime for El_gamal

```
p = next_prime(2^100); p
```

```
1267650600228229401496703205653
```

```
a=mod(primitive_root(p),p); a # the primitive root
```

```
2
```

```
A = randint(1,p); A # choose random integer
```

```
1221263409812795204699671326426L
```

```
B = a^A; B # get the public key
```

```
822744056685477525851982753735
```

```
# Assume message is
m = 10^30
# message should be less than p
m<p # verify message is less than p
```

```
True
```

```
k = randint(1,p); k # generate random integer
```

```
688305175663146651289207717570L
```

```
C = [a^k,B^k*m]; C # compute C a vector containing c1 and c2
```

[339977244045178702883272985111, 431008146133790869791862653462]

```
C[1]/C[0]^A # to decrypt
```

10000000000000000000000000000

Diffie Hellma Illustrated

```
p = next_prime(2^100); p # choose a prime
```

1267650600228229401496703205653

```
g=mod(primitive_root(p),p); g # get the primitive root pf the prime
```

2

```
a = randint(1,p); a # generate random integer # Alice gets a random
number which is her key
```

1217072149888585556421059143612L

```
A = g^a; A # she computes her public key like this and sends to Bob
```

503737370591877495834822980736

```
b = randint(p//2,p); a # generate random integer #  Bob also gets
his own random key
```

1217072149888585556421059143612L

```
B = g^b;B # he computes his public key and send to Bob
```

784245893844397310280880115604

```
B^a # Alice getting Bob public key computes B^a which is given
below. Alice and Bob now share a common key
```

550352812630842801429863176159

```
A^b # Bob also receiving Alice public key and computes A^b which
gives same value as that of Alice. So they now share a common key
```

550352812630842801429863176159