In [1]:
```
n = 12
Zn = IntegerModRing(n)
Zn
```

Out[1]:
```
Ring of integers modulo 12
```

In [2]:
```
list(Zn)
```

Out[2]:
```
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]
```

In [5]:
```
srr12 = [a for a in Zn if gcd(a, n)==1]
srr12
```

Out[5]:
```
[1, 5, 7, 11]
```

In [6]:
```
p = 13
```

In [7]:
```
Zp = IntegerModRing(p)
```

In [8]:
```
srr = [a for a in Zp if gcd(a, p)==1]
srr
```

Out[8]:
```
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
```

In [11]:
```
[Zp(a)^12 for a in srr]
```

Out[11]:
```
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
```

In [13]:
```
Zp(3)^6
```

Out[13]:
```
1
```

In [16]:
```
[(Zp(2)^k, k) for k in range(1, 13)]
```

Out[16]:
```
[(2, 1),
 (4, 2),
 (8, 3),
 (3, 4),
 (6, 5),
 (12, 6),
 (11, 7),
 (9, 8),
 (5, 9),
 (10, 10),
 (7, 11),
 (1, 12)]
```

In [18]:
```
p = random_prime(2^32, lbound=2^31)
p
```

Out[18]:
```
3129543419
```

In [19]:
```
Zp = IntegerModRing(p)
Zp
```

Out[19]:
```
Ring of integers modulo 3129543419
```

In [20]:
```
is_prime(p)
```

Out[20]:
```
True
```

In [21]:
```
Zp.is_field()
```

Out[21]:
```
True
```

In [22]:
```
r = Zp.multiplicative_generator()
r
```

Out[22]:
```
2
```

In [23]:
```
r.multiplicative_order()
```

Out[23]:
```
3129543418
```

In [24]:
```
p-1
```

Out[24]:
```
3129543418
```

In [25]:
```
b = Zp.random_element()
b
```

Out[25]:
```
2211351157
```

In [26]:
```
discrete_log?
```

In [27]:
```
discrete_log(b, r)
```

Out[27]:
```
862673043
```

In [28]:
```
r^862673043
```

Out[28]:
```
2211351157
```

Diffie-Hellman

In [29]:
```
Zp
```

Out[29]:
```
Ring of integers modulo 3129543419
```

In [30]:
```
r
```

Out[30]:
```
2
```

Alice escolhe um parâmetro a. Bob escolhe um parâmetro b.

In [31]:
```
type(r)
```

Out[31]:
```
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_gmp'>
```

In [32]:
```
a = randint(2, p-1)
b = randint(2, p-1)
```

In [ ]:
```
a, b
```

Out[32]: (2955053993, 229548920)

In [33]:
```
A = r^a # Alice envia A para Bob
```

In [34]:
```
B = r^b # Bob envia B para Alice
```

In [35]:
```
B^a # Alice recebe B de Bob e calcula B^a
```

Out[35]: 12152920

In [37]:
```
A^b # Bob recebe A de Alice e calcula A^b
```

Out[37]: 12152920

ElGamal

In [38]:
```
Zp, r
```

Out[38]: (Ring of integers modulo 3129543419, 2)

In [39]:
```
a = randint(2, p-1)
a
```

Out[39]: 362762259

In [40]:
```
b = r^a
```

In [41]:
```
PubKey = (p, r, b)
PrivKey = a
```

In [42]:
```
mens = 1234
```

In [48]:
```
k = randint(2, p-1)
gama = r^k
delta = mens*b^k
cif = gama, delta
cif
```

Out[48]: (3001266768, 2648251604)

In [49]:
```
(gama^a)^(-1)*delta
```

Out[49]: 1234

In [ ]:
```

```