

```
>>> p = 6619
>>> q = 9479
>>> n = p * q
>>> n
62741501
>>> f = (p-1)*(q-1)
>>> f
62725404
>>> f / 3.0
20908468.0
>>> f / 5.0
12545080.8
>>> e = 5
>>> d = 1
>>> while (e*d % f != 1):
...     d = d + 1
```

p and q are two prime numbers

f and 5 doesn't divide evenly – no common factors – relatively prime

```
...
>>> d
12545081
>>> M = 1234567
>>> M**e % n
39897957L
>>> pow(M, e, n)
39897957
>>> C = pow(M, e, n)
>>> C
39897957
>>> pow(C, d, n)
1234567
```

M is original message, numerically

computes M^e modulo n

C is encrypted message (number)

decrypting message using private key pair (d, n)

```
>>> M = 42351359
>>> C = pow(M, e, n)
>>> C
39992556
>>> pow(C, d, n)
42351359
```

another example