$n=p*q$; p,q-primes. We will deal with the numbers of 28 bit length.
$p=3$; $q=5$; --> $n=15$; mod n. $\boldsymbol{Z}_{15}=\{0, 1, 2, ..., 14\}$; *mod 15.

Multiplication Tab.		Z15												
*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	14	13	12	11	10	9	8	7	6	5	4	3	2	1

gcd(2,15)=1

$2^{-1}=8 \bmod 15$ since
$2 \cdot 2^{-1} = 2 \cdot 8 = 1 \bmod 15$

$S_{MJ}=\{1,2,4,7,8,11,13,14\}$

$|S_{MJ}|=8.$

$\mathcal{Z}_n^* = S_{MJ}$

$gcd(2,15)=1$

$gcd(6,15)=3$

Exponent Tab.		**Z15**													
^	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4
3	1	3	9	12	6	3	9	12	6	3	9	12	6	3	9
4	1	4	1	4	1	4	1	4	1	4	1	4	1	4	1
5	1	5	10	5	10	5	10	5	10	5	10	5	10	5	10
6	1	6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	1	8	4	2	1	8	4	2	1	8	4	2	1	8	4
9	1	9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	1	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1	11	1
12	1	12	9	3	6	12	9	3	6	12	9	3	6	12	9
13	1	13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1	14	1

$\boldsymbol{Z}_{15}^*=\{1, 2, 4, 7, 8, 11, 13, 14\}$; $\boldsymbol{Z}_{15}^*=\{z \mid gcd(z,n)=1\}$ $|n| = 28$ bits ; $n=p \cdot q$

Z_{15}*={1, 2, 4, 7, 8, 11, 13, 14}; Z_{15}*={z | gcd(z,n)=1}
In this case ***z*** and ***n*** are relatively prime.
Multiplicative inverse elements mod n.
>> mulinv(8,15)
ans = 2

$|n| = 28$ bits ; $n = p \cdot q$
$|p| = |q| \sim 14$ bits
$p, q \sim 2^{14} \Rightarrow n = p \cdot q =$
$\cong 2^{14} \cdot 2^{14} = \cong 2^{28}$

>> p=genprime(14)
p = 12409
>> dec2bin(p)
ans = 11 0000 0111 1001
>> q=genprime(14)
q = 11959
>> dec2bin(q)
ans = 10 1110 1011 0111
>> n=p*q
n = 148399231
>> dec2bin(n)
ans = 1000 1101 1000 0110 0100 0111 >> f111
>> factor(n) = 11959 12409

Euler totient function **ϕ**(***n***): defines number of numbers **z** less than **n** that gcd(***z***,***n***)=1.
ϕ(***n***) = **ϕ** ≡ **fy**.
If ***n***=***p********q*** where ***p***,***q***-primes then **ϕ**(***n***) = **ϕ** = (***p***-1)*(***q***-1) ≡ **fy**.
Let ***n***=3*5=15 --> **ϕ**(***n***) = **ϕ** = (3-1)*(5-1) = 2*4 = 8 ≡ **fy**.

Euler theorem. If gcd(***z***,***n***)=1 then

$$z^{\phi} = 1 \bmod n$$

$z^{\phi} = 1 \bmod n$ & $z^{0} = 1 \bmod n$
$\Downarrow$
Then $\phi \equiv 0$ computing exponents mod n
$\Downarrow$
The expression in the exponents can be reduced mod ϕ:
gcd(z,n) = 1, then
$z^{a(b+c)} \bmod n =$
$= z^{a(b+c) \bmod \phi} \bmod n.$

Exponents of numbers in Z_n are computed mod **ϕ**.
>> fy=(p-1)*(q-1)
fy = 148374864
>> m=1234567
>> e=2^16+1
e = 65537   % **e** computation according to RSA standard
>> isprime(e)
ans = 1
>> gcd(e,fy)
ans = 1

>> c=mod_exp(m,e,n) $c = m^{e} \bmod n$
c = 96879544

```
>> c=mod_exp(m,e,n)
c = 96879544
```

$c = m^e \bmod n$

$= z^{a(b+c) \bmod \phi} \bmod n.$

$z \in \mathcal{Z}_n^* = \{z \mid \gcd(z,n)=1\}$

```
>> d=mulinv(e,fy)          % verify if e*d=1 mod fy
d = 24783857
>> mod(e*d,fy)
ans=1
```

$s = m^d \bmod n$

```
>> s=mod_exp(m,d,fy)
s = 56547297

>> z1=mod_exp(c,d,n)
>> z2=mod_exp(s,e,n)
```

$z_1 = c^d \bmod n = (m^e)^d \bmod n =$

$= m^{ed \bmod \phi} \bmod n = m^1 \bmod n = m$

$z_2 = s^e \bmod n = (m^d)^e \bmod n =$

$= m^{de \bmod \phi} \bmod n = m^1 \bmod n = m.$