```
> restart;
> interface(warnlevel = 0): # Maple 12
> with(RandomTools):
```

Encryption/Decryption worksheet

```
> public := proc(N);        # random prime number; the public key
                local i;
                i := 0;
                while not(isprime(i)) do  # prime number 1 ≤ x ≤N-1
                i := Generate(integer(range = 1..N − 1))
                end do;
                return i;
              end proc:
```

```
> invmod := proc(p, Φ)   # modular inverse using Maple's igcdex(). See Egcd.mw
                local gcd, inv, x;
                if Φ > p then gcd := igcdex(p, Φ, 'inv', y) end if;
                if Φ < p then gcd := igcdex(p, Φ, 'x', 'inv') end if;
                if (gcd ≠ 1) then return 0 end if; # if gcd(x,N) ≠1 return 0
                if (inv < 0) then inv := inv + Φ end if;
    # return positive integer; a positive mod inverse
                return inv;
              end proc:
```

Seven digit message to be encrypted

```
> t := 8675309;
```

$$t := 8675309 \quad (1)$$

Generate random (pseudorandom) prime numbers p and q

```
> randomize( ):
  p := prevprime(Generate(integer(range = 3000 .. 5000)));
  q := nextprime(Generate(integer(range = 3000 .. 5000)));
```

$$p := 3391$$
$$q := 3079 \quad (2)$$

The product of the random numbers p and q

```
> N := p · q;
```

$$N := 10440889 \quad (3)$$

The product of the random numbers p-1 and q-1

```
> Φ := (p − 1)·(q − 1);
```

$$\Phi := 10434420 \quad (4)$$

Random prime number 1 < x < N-1
gcd(x, Φ) =1

```
> x := public(Φ); # public key
  'gcd(x, Φ)' = igcd(x, Φ);
```

$$x := 6262933$$
$$gcd(x, \Phi) = 1 \quad \textbf{(5)}$$

The modular inverse y is determined using Maple's igcdex(); the Extended Euclidean algorithm.

```
> y := invmod(x, Φ);    # secret key
  ' x·y mod Φ ' = x·y mod Φ;
  'gcd(x·y, Φ)' = igcd(x·y, Φ) ;
```

$$y := 72277$$
$$x\,y \bmod \Phi = 1$$
$$gcd(x\,y, \Phi) = 1 \quad \textbf{(6)}$$

Generating the encrypted message

```
> te := (t)^x mod N;
```

$$te := 4187871 \quad \textbf{(7)}$$

Decrypting the message

```
> td := (te)^y mod N;
```

$$td := 8675309 \quad \textbf{(8)}$$