```
(* RSA (Rivest-Shamir-Adleman) cryptosystem
Firstly we will encript a credit card number 5613
 7024 3798 6943 by the public key (n,e). Secondly we will
 find a private key d and decript the credit card number. *)
```

In[11]:=
```
(* public key *)
n := 1 000 001;
e := 13;
```

In[13]:=
```
(* prime factorization of n *)
FactorInteger[n]
```

Out[13]= {{101, 1}, {9901, 1}}

In[18]:=
```
(* n=pq *)
p := 101;
q := 9901;
```

In[20]:=
```
(* L *)
L := LCM[p - 1, q - 1];
L
```

Out[21]= 9900

```
(* prime factorization of L *)
FactorInteger[L]
```

Out[22]= {{2, 2}, {3, 2}, {5, 2}, {11, 1}}

```
(* de-kL=1 *)
{g, {d, k}} = ExtendedGCD[e, L]
```

Out[24]= {1, {-1523, 2}}

In[26]:=
```
(* d *)
d := -1523 + L
d
```

Out[27]= 8377

```
(* encryption of 5613 7024 3798 6943*)
Mod[{5613^e, 7024^e, 3798^e, 6943^e}, n]
```

Out[28]= {675 406, 911 491, 446 624, 644 570}

In[30]:=
```
(* decryption of 675406 911491 446624 644570 *)
Mod[{675 406^d, 911 491^d, 446 624^d, 644 570^d}, n]
```

Out[30]= {5613, 7024, 3798, 6943}