

RSA Coding Scheme Simulation

For the simulation of the RSA coding system, the following system was used to convert letters into numbers.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space	

The RSA coding system works with the concept of public key codes, where the method of how to encode a message is public and **anyone** can encode messages. The ability to decode is private (**Joe had the private key**), which only the person with the secret key will have the ability to decode.

Encoding – Public Key Code

Joe was sent a secret message that was created using the following public key:

$$n = 91 \text{ and } r = 5$$

The n is a number that is a product of two primes, which in the actual application of RSA coding would have been two huge prime numbers (three hundred digits). For the simplicity of our example and computing power, we used $n = 91$.

The r is a number relatively prime to $m = (p-1)(q-1)$, where p and q are the primes multiplied to calculate n . (Cannot calculate r without knowing the factorization of the number n , hence the importance of large primes which are virtually unfactorable even by the world's fastest computers)

The n and r become the public key code, and encoding messages follows the following process:

$$E \equiv L^r \pmod{n}$$

E = Encrypted number for the secret message (ours were all 2 digit numbers)

L = A number representing letters in the original message (ours were all 2 digit numbers)

n and r were the public key.

Example: 03 represents the letter D, so if I want to send the letter D secretly, I will use $E \equiv L^r \pmod n$ with our $n = 91$ and $r = 5$.

$$61 \equiv 03^5 \pmod{91}$$

So the number 61 will be sent as the encrypted number where Joe is the only person who knows the private key which will decode the message.

Decoding - Private

In order for Joe to decode the message, he had to know the private key, which in this case is $s = 29$. The process Joe used to decode the message was as follows.

$$L \equiv E^s \pmod n$$

E = A two digit number in the encrypted message

L = A two digit number representing a letter in the original message

n is the part of the public key code

s is the private number that Joe must know in order to decode the message. It is calculated based on other important knowledge about the numbers n and r . To calculate n , one must know how to factor n . In our case n is small and easy to factor, but the actual application of RSA coding will see n be the product of two huge primes. This makes n essentially unfactorable, even by the fastest computers in the world.

Calculating s :

Here is the process Joe used to calculate the private key - s .

1. Calculate m , where $m = (p-1)(q-1)$

- p and q are the prime factors of n

2. Calculate k , where $r^k \equiv 1 \pmod m$

- r is part of the public key where it is a number relatively prime to m .

3. $s \equiv r^{k-1} \pmod m$

In our example $n = 91 = (13 \cdot 7)$ and $r = 5$

1. $m = 12 \cdot 6 = 72$

$$2. r^k \equiv 1 \pmod{m} \rightarrow 5^6 \equiv 1 \pmod{72} \rightarrow k = 6$$

$$3. s \equiv r^{k-1} \pmod{m} \rightarrow s \equiv 5^{6-1} \pmod{72} \rightarrow s = 29$$

Example: Joe receives the number 61 and decodes the message, so he will use $L \equiv E^s \pmod{n}$ knowing $s = 29$.

$$L \equiv E^s \pmod{n} \rightarrow L \equiv 61^{29} \pmod{91} \rightarrow L = 03$$

Joe is able to decode the number 61 as 03, which is the letter D under our system.

RSA Real World Application

- Relatively new system of cryptography – Developed at MIT in 1978
- RSA – (Ronald Rivest, Adi Shamir, and Leonard Adleman)
- Technology based because of the need to compute with large numbers
- Primes are now extremely valuable (\$)
- RSA is widely used in electronic commerce protocols (I.E. - Online Shopping, Online Banking, Email, etc.)
- A gigantic string can be encoded and decoded at once provide a large enough n value hence the importance of computers for computation (our example $n = 91$, so we could only encrypt/decrypt a two digit string)
- For practical applications n will be a huge number – product of three hundred digit primes