RSA

Catherine Easton

July 2007

VIGRE REU at the University of Chicago, Apprentice Program

Abstract

This paper examines the mathematics of the RSA code through a simple example.

Contents

1 A Brief Introduction to Cryptography

In the classical explanation of cryptography, Alice wishes to write a message to Bob, but Eve continues to intercept her messages. Alice and Bob decide to encrypt their messages.

Alice and Bob can meet in person and exchange a key. With this information, they can both encrypt and decrypt messages to each other. Even if Eve manages to intercept a message, she will not be able to gain any information from it, seeing as it is encoded and she does not know the key necessary for decryption. This scenario uses private-key cryptography.

Now, however, let us assume that it is impossible for Alice and Bob to meet, and that they are therefore unable to exchange the key. Obviously, Alice cannot send Bob the key, seeing as their messages are being intercepted by Eve, who would then know the key as well. To overcome this barrier, Alice and Bob must use public-key cryptography. Bob selects both an encryption function and a corresponding decryption function. He sends only the encryption function to Alice.

She then uses the encryption function to encrypt her message. Once her message is encrypted, Alice herself is unable to decrypt it. She then sends the message to Bob, who is the only one able to decrypt it. Assuming Eve intercepted Bob's message and learned the encryption function, she is in the same position as Alice: knowing both the encryption function and the encrypted message, she remains unable to decrypt it. This scenario uses public-key cryptography.

RSA is one example of an algorithm for public-key cryptography, discovered in 1977 by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman.

2 RSA

2.1 Keys needed in RSA

RSA's public key is used for encrypting messages. Messages encrypted with this public key must then be decrypted using a private key. Below are the steps that one must follow in order to obtain a public and private key.

1. Let p and q be two random large prime numbers of one's choice.
2. Calculate $n = pq$
3. Calculate $\phi(n) = (p-1)(q-1)$
4. Choose an integer e such that:
   (a) $1 \leq e \leq \phi(n)$
   (b) e and $\phi(n)$ are coprime
5. Find d such that $ed \equiv 1(mod \ \ \phi(n))$

The public key consists of n and e (for encryption).
The private key consists of n and d (for decryption).

2.2 RSA Encryption

To begin using RSA, each letter of the alphabet must be associated its own number. However, using the letter's position in the alphabet (A = 1 ... Z = 26) would mean some letters were being coded by one-digit numbers, and others by two-digit numbers. The message would not be able to be decrypted. Therefore, each letter is associated with a two-digit number.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Let's encrypt 'Math'

M	A	T	H
22	10	29	17

Therefore, the numeric message is 22102917.

Let $p = 11$

and $q = 17$

In this example of RSA encryption, we will use primes with small values for simplicity. However, when aiming for a secure code, the larger the primes the better.

$n = pq = 11 * 17 = 187$

Now, we will divide the numeric message into segments. Each segment must be the largest number possible, all the while remaining lesser than n, therefore lesser than 187.

S_1= 22 $S_2 = 102$ $S_3 = 91$ $S_4 = 7$

$\phi(n)$ =(p-1) (q-1)= $(11-1)(17-1) = 10 * 16 = 160$

$\phi(n)$ *must not be divulged if the code is to remain secure.*

Let $e = 7$
This fulfills both of the restrictions on choosing an e:
$1 \leq e \leq \phi(n)$ and e and $\phi(n)$ are indeed coprime.

The public key (n, e), is in this case (187 , 7).

Let S denote a segment of the message such that $1 \leq$S$\leq$n-1
$E(S)$ denotes the encryption of S
$E(S) = S^e$ *(mod n)*

Therefore:

$E(S_1) = 22^7 \ (mod \ \ 187) = 44$
$E(S_2) = 102^7 \ (mod \ \ 187) = 119$
$E(S_3) = 91^7 \ (mod \ \ 187) = 31$
$E(S_4) = 7^7 \ (mod \ \ 187) = 182$

Let $E(m)$ denote the encryption of the entire message.
$E(m) = E(S_1) + ES_2) + ... + E(S_4)$
$E(m)$= 44 119 31 182

2.3 RSA decryption

We use d, the number such that

$ed \equiv 1 \ \ (mod \ \ \phi(n)) \ \ and \ \ 1 \leq$e$\leq \phi(n)$

$$\Leftrightarrow ed - 1 = k * \phi(n) \tag{1}$$

The value of e was publicized.
However, only the person for whom the message is intended knows the value of $(p-1)(q-1) = \phi(n) = 160$

Therefore, the person for whom the message is intended can plug these values into the equation (1) and obtain:
$7d - 1 = 160k$

However:

$$160 = 7 * 22 + 6 \Leftrightarrow 6 = 160 - 7 * 22 \tag{2}$$

$$1 = 7 - 6 \tag{3}$$

From the equations (2) and (3):

1 = 7 - (160 - 7*22)
$\Leftrightarrow 1 = 7 * 23 - 160$
$\Leftrightarrow 7 * 23 - 1 = 160 \;\; where:$
$7 = e \quad 23 = d \quad 160 = \phi(n) \;\; and \;\; k = 1$
$ed \equiv 1 (mod \;\; \phi(n))$

The private key (n, d), is in this case (187 , 23).

Let $T_i = E(S_i)$
$D(T)$ denotes the decryption of T

$D(T) = S^d \quad (mod\ n)$

Therefore,
$D(T_1) = 44^{23}(modn) = 22$
$D(T_2) = 102$
$D(T_3) = 91$
$D(T_4) = 7$

The deciphered message is 22102917.
One knows that each letter corresponds to a two-digit number.
$22 \rightarrow M$
$10 \rightarrow A$
$29 \rightarrow T$
$17 \rightarrow H$

The message 'Math' has been decoded.