WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 8

May 7, 2024

Table of Contents i

1 Introducing the RSA algorithm

Definition 1

Suppose I want you to learn a plaintext (original message). I will send you a ciphertext or encryption, from which you will learn the plaintext. Creating the ciphertext from the plaintext is called encryption and it uses encryption key. Creating the plaintext from the ciphertext is called decryption and it uses a decryption key.

Suppose I want to send you a plaintext, I use your public key, which is advertised by you, to encrypt the plaintext and then send it to you via an unsecured channel. You then decrypt the data using your private key, which is known to you only.
The RSA algorithm, allows a message to be encrypted without the sender knowing the key.

The RSA assumption is that it is easy to find two large prime numbers but hard to factor a large composite number into its prime factorization form.

HOW it works

Let's say I want to send you an encrypted message.
To do this, you need to make a public key, which comprises two numbers and make public.

First, you choose two prime numbers: Let's say 11 and 17. In calculations, we call these numbers p and q such that $p \neq q$.

You keep p and q private.

Multiply p and q to get 187. Let's call this value m - it's one of your public key numbers.

Then find $\phi(m) = (p-1)(q-1)$ and keep it private. In our case it will be $\phi(m) = 160$

Your second public number is e, which you can choose such that $1 < e < \phi(m)$ and e is coprime to $\phi(m)$.

Let's say you pick 7. Compute the private exponent d such that, $1 < d < \phi(m)$ and that $ed \equiv 1 (\mathrm{mod}\, \phi(m))$. In our case $d = 23$

Now publish m and e wherever you like. Keep p, q, d and $\phi(m)$ private.

How to encrypt a message

Now I'm going to send you a message outlining how many Number theory text books are in my library. Let's say they are 99. But we don't want anyone else to know. This is the plaintext. Remember that the plaintext x should be a number that lies in the range $1 < x < m - 1$.

(Even if the message isn't a number, it can easily be represented as one)

I look you up on a directory and find your public key - your m and e. In our case they are 187 and 7.

Then the calculations start. I raise my message to e
In other words, I multiply $99 \times 99 \times 99 \times 99 \times 99 \times 99 \times 99$ (seven times) and end up with 99^7.
I then reduce this number modulo n. That is, find $99^7 \bmod 187$.

In our encryption example, $99^7 \bmod 187 = 176$. And it's this number that I send to you; that's our encrypted message. We don't care if it's intercepted, because only you can decipher it.

How do you then decrypt it

But how do you decrypt 176 to get my real message, 99?

You then take my message (176) and multiply it by itself 23 times. That is 176^{23} and divide m $(187$, the product of your original primes p and $q)$ and find the remainder.

That is, find $176^{23} \bmod 187$. You will find that $176^{23} \bmod 187 = 99$ -which my original message.

There you have it: an encrypted, then decrypted, message.

Anyone can send you a message using your public key.

Note that in real encryption, you'd never choose simple prime numbers like 11 and 15 as p and q. You'd go for much larger primes, hundreds or maybe thousands of digits long.

Algorithm 1 (RSA Key generation algorithm:- Summary)

Suppose you want to send some text x to your friend.

1. Your friend Selects two prime numbers p and q such that $p \neq q$ and calculates $m = p \times q$.
   Note that m will be a public key while p and q will be kept private.
2. The friend calculates $\phi(m) = (p-1)(q-1)$
3. The friend chooses an integer e (the encryption key) such that, $1 < e < \phi(m)$ and e is coprime to $\phi(m)$.
   Note that e will be another public key.
4. The friend computes the d (the decryption key) such that, $1 < d < \phi(m)$ and that $ed \equiv 1 (\mathrm{mod}\, \phi(m))$.
   Note that d will be a private key.
5. The friend sends you the public key (m, e) and keeps p, q, d and $\phi(m)$ private.

Algorithm (Conti...)

RSA Encryption

1. On receiving the encryption key (m, e), let the plaintext x be treated as a number to lie in the range $1 < x < m - 1$.
2. The ciphertext corresponding to x is $y = x^e \bmod m$
3. Send the ciphertext y to your friend.

RSA Decryption

1. Your friend receives y from you and uses the private key (m, d).
2. Computes the $x = y^d \bmod m$.

Example 1

Alex chooses the two primes $p = 11$ and $q = 17$ and computes $n = 11 \times 17 = 187$. He chooses $e = 7$ and computes the inverse $d = 23$ of $7 \bmod 160$. The encryption key is $(187, 7)$, the decryption key is $(187, 23)$.

Wanjiru wants to encrypt the message $w = 91$. She knows Alex's encryption key. She computes $c = 91^7 \bmod 187 = 31$ and sends it to alex.

Alex computes $31^{23} \bmod 187 = 91$ and recover's Waniiru's original text.

Example 2

Ochieng' knows Alex's encryption key in example 1 above. He wants to send Alex the word "NO". He changes every letter to a number (from 00 to 25), with each coded as two digits. Concatenates the numbers to get the plaintext 1314. Since this number is bigger than $n-1$, he breaks it into two digits to have $13, 14$.

Next using fast powering algorithm he computes the following

$$13^7 \equiv 106 \bmod 187, \quad 14^7 \equiv 108 \bmod 187$$

and sends Alex the encrypted message $106,\ 108$.
Alex computes $106^{23} \equiv 13 \bmod 187, \quad 108^{23} \equiv 14 \bmod 187$

and now using the number-to-letter substitution table for the final decryption step

13	14
N	O

supplying the obvious word breaks and punctuation, he reads "NO".

Example 3

Suppose you chose p and q as 7 and 11, then

$m = 7 \times 11 = 77$.

$\phi(m) = (7-1)(11-1) = 60$.

Then choose e, an integer less than 60 but relatively prime to 60.

Let us say you chose $e = 17$.

You then find the d such that $ed \equiv 1 \bmod \phi(60)$. That is, you find $e^{-1} \bmod 60$ using the extended Euclid's algorithm or the Euler's Theorem. Let us use Euler's Theorem,

$17^{-1} \bmod 60 = 17^{\phi(60)-1} \bmod 60 = 17^{15} \bmod 60$. Let us now use the fast powering algorithm

$$17^1 = 17, \quad 17^2 = 49, \quad 17^4 = 1$$

Now $15 = 4 \cdot 3 + 3$

Thus, $17^{15} = 17^3 = 17^{2+1} = 17^2 \times 17^1 = 49 \times 17 = 53$

Thus $d = 53$.

Example (conti...)

So, $7, 11, 60$ and 53 are kept secret. What is made public is 77 and 17.

Suppose the plaintext $x = 8$.

The ciphertext corresponding to x is $y = x^e \bmod m$. That is, $y = 8^{17} \bmod 77$. Using the fast powering algorithm we obtain $y = 57$. This is the ciphertext to be send.

To decrypt to obtain back the x we have $x = y^d \bmod m$.

That is, $x = 57^{53} \bmod 77$ which gives 8.

Example 4

Jennifer creates a pair of keys for herself. She chooses $p = 311$ and $q = 367$. She calculates $n = 311 \times 367 = 114137$. She then calculates $\phi(n) = 310 \times 366 = 113460$. She then chooses $e = 343$. Show how Ted can send a message "OK" to Jennifer if he knows e and n. Show how Jennifer would decrypt Ted's ciphertext.

Solution

Ted changes every letter to a number (from 00 to 25), with each coded as two digits. He concatenates the numbers and gets a four-digit number. The plaintext is 1410.

Ted then uses e and n to encrypt the message. The ciphertext is $1410^{343} \bmod 114137$. Using fast powering aligorithm we have;

Solution (Conti...)

$1410^1 = 1410$ $\quad$ $1410^{32} = 69420$

$1410^2 = 47771$ $\quad$ $1410^{64} = 43986$

$1410^4 = 13263$ $\quad$ $1410^{128} = 31909$

$1410^8 = 22052$ $\quad$ $1410^{256} = 82241$

$1410^{16} = 67084$

Thus, $1410^{343} = 1410^{256+64+16+4+2+1}$

$$= 1410^{256} \times 1410^{64} \times 1410^{16} \times 1410^4 \times 1410^2 \times 1410^1$$

$$= 25134 \times 43986 \times 67084 \times 13263 \times 47771 \times 1410$$

$$= 42533 \bmod 114137$$

Jennifer receives the message 42533 and uses the decryption key d to decrypt.

First she calculates d such that $ed \equiv 1 \bmod \phi(n)$

or $343d \equiv 1 \bmod 113460$

Solution (Conti...)

Let us use the division algorithm

$$113460 = 343(330) + 270$$
$$343 = 270(1) + 73$$
$$270 = 73(3) + 51$$
$$73 = 51(1) + 22$$
$$51 = 22(2) + 7$$
$$22 = 7(3) + 1$$
$$7 = 1(7) + 0$$

Using the extended Euclidean algorithm we obtain

$$1 = 343(15547) + 113460(-47) \text{ and so } d = 15547.$$

Jennifer decrypts as $42533^{15547} \bmod n = 42533^{15547} \bmod 114137$

Solution (Conti...)

Using the fast powering algorithm we obtain:

$$42533^{1} = 42533 \qquad 42533^{128} = 16372$$

$$42533^{2} = 98776 \qquad 42533^{1024} = 43728$$

$$42533^{8} = 35213 \qquad 42533^{2048} = 823$$

$$42533^{16} = 85138 \qquad 42533^{4096} = 106644$$

$$42533^{32} = 94722 \qquad 42533^{8192} = 103782$$

So that

$$\begin{aligned} 42533^{15547} &= 42533^{8192+4096+2048+1024+128+32+16+8+2+1} \\ &= 103782 \times 106644 \times 823 \times 43728 \times 16372 \times 94722 \times \\ &\quad 85138 \times 35213 \times 98776 \times 42533 \\ &= 1410 \end{aligned}$$

Interpret the resultant numbers again as letters to produce plaintext "OK".

Example 5

Now suppose you want to send the message "LOVEMATHS" to Jenipher using her public key in example 4 above. Encrypt the message. Also show how Jenipher would decrypt to obtain your message back.

Solution

Change every letter to a number (from 00 to 25), with each coded as two digits. Concatenate the numbers to get the plaintext $11142104120019 0718$. Since this number is bigger than $n-1$, we can break it into five digits or four digits or any number of digits that would give us numbers less that $n-1$. Let us break as follows encrypt.

$$11142, \quad 1041, \quad 2001, \quad 90718$$

Solution (Conti...)

Next we using fast powering algorithm we obtain the following

$$11142^{343} \equiv 18485 \bmod 114137$$
$$1041^{343} \equiv 16492 \bmod 114137$$
$$2001^{343} \equiv 64028 \bmod 114137$$
$$90718^{343} \equiv 39554 \bmod 114137$$

The encrypted message is the list of numbers

$$18485, \quad 16492, \quad 64028, \quad 39554$$

Jennifer decrypts the strings as

$$18485^{15547} \equiv 11142 \bmod 114137$$
$$16492^{15547} \equiv 1041 \bmod 114137$$
$$64028^{15547} \equiv 2001 \bmod 114137$$
$$39554^{15547} \equiv 90718 \bmod 114137$$

Solution (Conti...)

This gives her the string of digits

$$11142104120019 0718$$

and now using the number-to-letter substitution table for the final decoding step.

11	14	21	04	12	00	19	07	18
L	O	V	E	M	A	T	H	S

Supplying the obvious word breaks and punctuation, she reads “Love Maths”.