WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 21

June 6, 2024

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.

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

Let us say I want to send some ciphertext to Mugasia. Suppose she chooses two primes $p = 11$ and $q = 17$ and computes $n = 11 \times 17 = 187$ and $\phi(187) = (11-1)(17-1) = 160$.
Suppose she chooses $e = 7$. She is required to compute $d = e^{-1} \bmod 160 = 7^{-1} \bmod 160$. Let us use the extended Euclid's algorithm to do this.

$$160 = 7(22) + 6$$
$$7 = 6(1) + 1$$
$$6 = 1(6) + 0$$

Thus $\gcd(160, 7) = 1$. We solve for it.
$1 = 7 - 6(1) = 7 - [160 - 7(22)](1)$

$$= 7 - 160(1) + 7(22) = 160(-1) + 7(23)$$

Thus $d = 23 \bmod 160$. The encryption key is $(187, 7)$, the decryption key is $(187, 23)$.

Example (conti...)

I want to send her the message $w = 91$.

I use her encryption key which is public to encrypt w first.

I compute $c = 91^7 \bmod 187$ using fast powering algorithm

$$\begin{aligned}
91^1 &= 91 \\
91^2 &= 53 \\
91^4 &= 4 \\
\therefore 91^7 &= 91^4 \times 91^2 \times 91^1 \\
&= 4 \times 53 \times 91 = 31 \bmod 187
\end{aligned}$$

I send her the ciphertext 31.

To decrypt she computes $31^{23} \bmod 187$ using fast powering algorithm.

Example (conti...)

$$
\begin{aligned}
31^1 &= 31 \\
31^2 &= 26 \\
31^4 &= 115 \\
31^8 &= 135 \\
31^{16} &= 86 \\
\therefore 31^{23} &= 31^{16} \times 31^4 \times 31^2 \times 31^1 \\
&= 86 \times 115 \times 26 \times 31 = 91
\end{aligned}
$$

Example 2

Now suppose that I want to send to Mugasia the word "NO". I would still use her public key in example 1. I change every letter to a number (from 00 to 25), with each coded as two digits. Concatenate the numbers to get the plaintext 1314. Since this number is bigger than $n-1$, I break it into two digits to have $13, 14$.

Next using fast powering algorithm I compute the following

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

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

and now uses 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".

Revision Question 1

Using RSA algorithm, if $p = 7$ and $q = 13$ and $e = 7$. Find d and a cipher value of $x = 8$. Decrypt the ciphertext.

Solution

Solution

Revision Question 2

Using RSA algorithm, if $p = 5$ and $q = 17$ and $e = 7$. Find d and a cipher value of $x = 6$. Decrypt the ciphertext.

Solution

Solution

Revision Question 3

Using RSA algorithm, if $p = 3$ and $q = 11$ and $e = 7$. Find d and a cipher value of $x = 5$. Decrypt the ciphertext.

Solution

Solution

Revision Question 4

Using RSA algorithm, if $p = 5$ and $q = 11$ and $e = 3$. Find d and a cipher value of the word "LOVE". Decrypt the ciphertext.

Solution

Solution

Revision Question 5

Using RSA algorithm, if $p = 3$ and $q = 13$ and $e = 7$. Find d and a cipher value of $x = 9$. Decrypt the ciphertext.

Solution

Solution

Revision Question 6

Using RSA algorithm, if $p = 7$ and $q = 11$ and $e = 3$. Find d and a cipher value of $x = 5$. Decrypt the ciphertext.

Solution

Solution

Revision Question 7

Using RSA algorithm, if $p = 7$ and $q = 17$ and $e = 5$. Find d and a cipher value of the word "HATE". Decrypt the ciphertext.

Solution

Solution