16 (~~17~~) September, 2024

RSA
Concept of coprime (relatively prime)
Concept of numbers that are the multiplicative inverse of each other
RSA Examples

RSA

- Invented by Ron Rivest, Adi Shamir, and Len Adleman at MIT 1978
- Block size can be variable
- Key length can be variable
- Plaintext must be smaller than the key length
- Ciphertext block will be the length of the key
- Product of prime numbers, factoring of result

→ Applications: secrecy(secret exchange of keys) and digital signature

RSA is based on the reality that calculating n (a product of two prime numbers p and q is easy, whereas finding two prime factors p and q from n is extremely difficult)

Coprime (or relatively prime)

Two numbers are co-prime if the greatest common divisor (GCD) between them is only 1.

- A and B are coprime iff gcd(A,B) = 1.
- For example, 6 and 11. The GCD between **6** & **11** is 1 only (factors of **6** are 2, 3 and 1 and factors of **11** are 11 and 1).

Note: It isn't necessary that the two numbers are prime! They have to be prime to each other.

Euler Totient Function

If n is a positive integer, φ(phi) function counts all the positive integers less than n that are relatively prime to n.

φ(n) = Totient(n) = numbers of integers less than n that are coprime to n

φ(10) = 4
Because these four numbers → (1,3,7,9) are all coprime to 10, and are smaller than 10

Note: Generally, φ(p) = (p-1) where p is a prime number

Multiplicative Inverse

Multiplicative Inverse of a number X is Y iff Y multiplied with X yields 1.

For example, X * Y = 1, Both X and Y are the multiplicative inverses of each other.

Do keep in mind, we will be assuming modular arithmetic (read up on modular arithmetic here).

PKC (Public Key Cryptography) -- how does it work?

Plaintext M and ciphertext C are integers between 0 and n-1 (n is the product of two prime numbers).

Key$_1$ = {e, n}, Key$_2$ = {d, n}

Where **e** and **d** are two secret number

$C = M_e \bmod n$ ← this is the encryption, done at the sender side

$M = C_d \bmod n$ ← this is the decryption, done at the receiver side

RSA Key Construction

Select two large primes: p, q, $p \neq q$

$n = p*q$

Calculate Euler's Totient Function, $\varphi(n) = (p-1)(q-1)$ ← *I did not prove this*

Select e relatively prime to φ => $GCD(\varphi,e) = 1$; $0 < e < \varphi$ ← find e that is coprime of φ

Calculate d = inverse of e mod φ => $d * e \bmod \varphi = 1$ ← d is the multiplicative inverse of e

public key = (e, n)
private key = (d, n)

The roles of e & d are interchangeable. i.e. $(x^d)^e \bmod n = (x^e)^d \bmod n$

RSA Examples

EXAMPLE 1:

Assume p=5, q=11
n = p*q = 5 * 11 = 55 (*we can advertise this*)

Find e?

$\varphi(n) = (p-1)(q-1) = 4*10 = 40$

We need e such that e is coprime of 40. 40 has factors: 2, 5, 1.

So, e=3 will work for us. GCD(3, 40) = 1

Let people know about (e, n)

Assume our plaintext is **M=7** (sender's original message)

I receive: $C = M^e \pmod n = 7^3 \pmod{55} = 343 \bmod 55 = 13$

So, ciphertext **C = 13**

I need to solve $d*e = 1 \bmod \varphi$

We can also write this as: $d*e \pmod \varphi = 1$

So, $d*3 \pmod{40} = 1$

Using simple hit and trial, we see that the possible solutions to the RHS (right hand side) are 1, 41, 81, 121, etc, i.e., 40k+1. But we need that answer which is divisible by 3, since d should be a whole number. 81 fits this requirement.

$3d = 81 = 1 \bmod 40$
$D = 81/3 = 27$

Then finally,

$M = C^d \pmod n = 13^{27} \pmod{55} = 7$

To solve for such large exponents, you may use the modular exponentiation calculators available online, for example, here.

EXAMPLE 2:

Select two large primes: $p, q, p \neq q$

$p = 17, q = 11$

$n = p*q = 17*11 = 187$

Calculate $\varphi = (p-1)(q-1) = 16*10 = 160$

Select e, such that gcd(φ, e) = 1; 0 < e < φ say, e = 7

Calculate d such that d*e mod φ = 1

Use Euclid's algorithm to find $d=e^{-1}$ mod φ

160k+1 = 161, 321, 481, 641

Check which of these is divisible by 7

161 is divisible by 7 giving d = 161/7 = 23

Key_1 = Public key = {7, 187}, Key_2 = Private key = {23, 187}

EXAMPLE 3:

We also solved for p=23 and q=41

We chose e=7, and M=35.

Here, n will be 943

We found C to be 545.

Φ in this case was 880.

Final Note:

We have shown examples with smaller primes, but keep in mind that, in today's world, we will be dealing with prime numbers with more than 100 digits, otherwise RSA might not provide the desired security.