Ziaur Rahman , 124606 <zia@iut-dhaka.edu>

RSA Basics - Rahman Ziaur

Rahman Ziaur <rahman.ziaur@rmit.edu.au> Tue, Oct 8, 2019 at 1:40 PM
To: zia <zia@iut-dhaka.edu>, ziarajbari <ziarajbari@hotmail.com>, ziarajbari <ziarajbari@gmail.com>

----------RSA BASICS ----------

Integer:

An integer is a number that can be written without a fractional component. For example, 21, 4, 0, and −2048 are integers, while 9.75, 5, and √2 are not.

Modular arithmetic:

It is a special type of arithmetic that involves only integers, where integers "wrap around" when reaching a certain value called the ***modulus.***
For example, in a clock 13:00 becomes 1:00, 14:00 becomes 2:00, and so on.

So, 13 ≡ 1 mod 12, read as "13 congruent to 1 mod 12, similarly 38 ≡ 2 mod 12 as 38 ≡ 3 x 12 + 2.

In our security study, we deal with prime integers within a certain modulo.

Prime Integer:

A Prime Number is a whole number greater than 1 that can not be made by multiplying other whole numbers. Example: 2, 3, 5, 7, 11, 13, 17, 19 and 23 are prime numbers.

Prime Factorisation:

"Factors" are the numbers you multiply together to get another number. For example, 2 and 3 are the factor of 6 as 2 X 3 = 6.

Writing a number as a product of prime numbers is called a prime factorisation of the number. For example, 2 and 3 are the prime that can produce 12 through multiplication such as 12 = 2 × 2 × 3.

GCD:

Greatest common divisors (GCD) of two numbers can be calculated by determining the prime factorisation.

For example, we can get the greatest common divisor (GCD) of 48 and 180 as below. Firstly, let's find the prime factorisation of 48 and 180:

48 = 2 × 2 × 2 × 2 × 3,
180 = 2 × 2 × 3 × 3 × 5.

Common factors are common is two "2"s and a "3". Therefore, GCD(48, 180) is = 2 × 2 × 3 = 12.

But, Calculating GCD by Prime Factorisation method seems time-consuming. We can do it by division and Euclidean method.

Euclidean Method:

1) Find the gcd (27, 33)?

Solution: Let's try to represent the bigger one '33' using the smallest one 27.

33 = 1 × 27 + 6 (let's again build 27 using 6)
27 = 4 × 6 + 3
6 = 2 × 3 + 0

Therefore, the gcd is 3.

However, GCD using the *Successive Division Method* seems easier that others.

Example: Find gcd(24,18)

Let's larger number (24) as a dividend by the smaller number (18) as the divisor and divide. Then again divide the divisor (18) by the remainder (6). Repeat the process until we get the reminder '0'. The divisor that produces '0' at last is our desired gcd.

```
18 | 24 | 1
     18
    ---
     6 | 18 | 3
         18
        ---
          0
```

Co-prime:

Two integers *a* and *b* are said to be Co-prime if the gcd (a,b) = 1. That means they have no common factors other than 1.

Example:

21 and 22 are coprime. Factors of 21 are 1, 3, 7 and 22 are 1, 2, 11 and 22. The only common factor is 1.

Similarly, 21 and 24 are NOT coprime. The factors of 21 are 1, 3, 7 and 21 and 24 are 1, 2, 3, 4, 6, 8, 12 and 24. The common factors are 1 AND 3. So they are not coprime to each other.

We can find Euler's Totient of a number by using this co-prime concept.

Euler's Totient:

The Euler's totient of a number n, written $\phi(n)$, is the number of relative primes to n which are less than n. For example, There are 24 coprime numbers of 35. They are 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34. All are less than 35. Therefore, we can say $\phi(35) = 24$.

It should be time-consuming to count all co-primes of a given number (as 35 or larger). Swiss Mathematician Euler solved this problem.

According to prime factorisation 35 can be represented by 5 and 7 as 35 = 5 × 7. We can count coprime of 35 using a formula (Eluer Totient), as 35 = (5 - 1) × (7 - 1) = 4 × 6 = 24 = ϕ (n). If 5 and 7 are replaced with two prime numbers p and q, then it becomes, ϕ (n) = (p-1)(q-1).

Euler proved *that if n* and *a* are coprime [gcd (n,a) = 1] positive integers, then $a^{\varphi (n)} \equiv 1 \pmod{n}$.

Example: if *n* = 10, φ(10) = 4 as coprimes are 1, 3, 7, 9. Here 11 is coprime with 10. Let's assume 11 as our *a.*

Therefore, $11^4 = 11^2 \times 11^2 = 121 \times 121 = 14641 \equiv 1 \bmod 10$.

Let's use this trick to find larger exponentiation.

For example, $55^4 \bmod 10 \equiv$?

From prime factorization, 55 = 5 × 11.

$\Rightarrow 55^5 = (5 \times 11)^5 = 5^5 \times 11^5 = 5^5 \times (11^4 \times 11^1) = 3125 \times 11 \times (11^4) \equiv 3125 \times 11 \times 1 \equiv 34375 \equiv 5 \pmod{10}$.

Euler Totient and Modular Arithmetic can be applied to generate a key pair which is the core concept of RSA cryptosystem.

RSA Cryptosystem:

In RSA, a message (M) is encrypted using a public key and decrypted using the private key. Two large prime numbers p and q work together to form the keys.

Let, n=p × q, find, (p -1) × (q - 1) = φ(n).

We have to pick e which is coprime to φ(n) such that 1 < e < φ(n) and gcd(φ(n), e) = 1.

Therefore, the public key is (n, e). Though n is public, difficulty in factorizing a large prime number ensures none can find two primes to obtain n in finite time which is the core strength of RSA.

Example:

If prime numbers p=3 and q=11. n = 3 × 11 = 33. Coprimes of 33 are 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32. That means φ(n) = 20.

That is how, (p - 1) × (q - 1) = (3 -1) × (11 - 1) = 2 × 10 = 20 = φ(n).

Now to pick the *e*, we have to again find a coprime of 20. The coprimes are 1, 3, 7, 9, 11, 13, 17, 19. Let's pick 7 as e. Therefore, the public key is (33, 7).

Now, let's find d, as if e × d ≡ 1 mod φ(n). We can find d from e as it is a small number.

$d \equiv e^{-1} \bmod \phi (n)$. One of the easiest ways of finding the modulo of an inverse number is to find the first number congruent 1 that is the multiple of that **inverse number** within the **modulo**.

$d \equiv e^{-1} \bmod \phi (n) \Rightarrow d \equiv 7^{-1} \bmod 20$. Congruent 1 in modulo 20 is 21, 41, 61…etc. The first one that is a multiple of 7 is 21 as it can be written 7 × 3 = 21. So, $1 \equiv 21 \bmod 20 \Rightarrow 3 \times 7 \bmod 20 \Rightarrow d \equiv e^{-1} = 7^{-1} \equiv \underline{\mathbf{3}} \bmod 20$. Therefore the private key is (d, p, q).

Encryption:

Public Key (n, e) = (33, 7). Let's assume our message (M) **3**.

Ciphertext, $C = M^e = 3^7 = 2187 \bmod 33 \equiv \mathbf{9} \bmod 33$.

Decryption:

Private Key (d, p, q) = (3, 3, 11) and n = 33.

Message, M = $C^d = 9^3 = 729 \bmod 33) \equiv \mathbf{3} \bmod 33$.
RSA is used to sign a digital message. The signing process includes producing a hash and encrypting the hash using the private key. Then the recipient can verify the message after decrypting that hash-cipher using the public key.

Thanks for your patience.

Rahman Ziaur
