RSA Public-Key Cryptography

- To create an RSA public/private key pair, here are the basic steps:

  1- Choose two prime numbers, p and q such that $p \neq q$.

  2- Calculate the modulus, $n = p \times q$.

  3- Calcuate $\phi(n) = (p-1) \times (q-1)$.

  4- Select integer e such that gcd ($\phi(n)$, e) = 1 and $1 < e < \phi(n)$. (* gcd is greater common divisor)

  5- Calculate an integer d from the quotient $de \equiv 1 \pmod{\phi(n)} \Rightarrow de = 1 + k\,\phi(n) \Rightarrow$

  $d = (1 + k\,\phi(n)) / e$
- To encrypt a message, M, with the public key (e, n), create the ciphertext, C, using the equation:

  $C = M^e \bmod n$
- The receiver then decrypts the ciphertext with the private key (d, n) using the equation:

  $M = C^d \bmod n$

- $n = pq$, where p and q are distinct primes.
- $\phi = (p-1)(q-1)$
- $e < n$ such that $\gcd(e, \phi) = 1$
- $d = e^{-1} \bmod \phi$
- $c = m^e \bmod n, 1 < m < n$
- $m = c^d \bmod n$

The RSA Example

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = p× q = 17 × 11 = 187.
3. Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose e = 7.
5. Determine d such that $de \equiv 1 \pmod{160}$ and d < 160. $de = 1 + k\,\phi(n)$

The correct value is d = 23, because 23 × 7 = 161 = 1 + (1 × 160).

The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}.

Given a plaintext input of M = 88. For encryption, we need to calculate $C = 88^7 \bmod 187$.

we can do this as follows.

$88^7 \bmod 187 = [(88^4 \bmod 187) * (88^2 \bmod 187) * (88^1 \bmod 187)] \bmod 187$

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$

$88^7 \bmod 187 = (88 * 77 * 132) \bmod 187 = 894{,}432 \bmod 187 = 11$

For decryption, we calculate $M = 11^{23} \bmod 187$:
$11^{23} \bmod 187 = [(11^1 \bmod 187) * (11^2 \bmod 187) * (11^4 \bmod 187) * (11^8 \bmod 187) * (11^8 \bmod 187)] \bmod 187$
$11^1 \bmod 187 = 11$
$11^2 \bmod 187 = 121$
$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$
$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$
$11^{23} \bmod 187 = (11 * 121 * 55 * 33 * 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$

In the preceding example shows, we can make use of a property of modular arithmetic:
$[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

As another example, suppose we wish to calculate $x^{11} \bmod n$ for some integers x and n. Observe that $x^{11} = x^{1+2+8} = (x)(x^2)(x^8)$.

Example: 2

1. Select two prime numbers, p=3 and q=11
2. Calculate n=pq=3*11=33
3. Calculate φ(n)=(p-1)(q-1)=(3-1)(11-1)
   =2*10=20
4. Select e such that e is relatively prime to φ(n)-20.
   So, we select e=7
5. Determine d such that ed=1 mod φ(n)
   7d=1 mod 20
   7*3=1 mod 20
   21=1 mod 20
   (d is calculated using extended Euclid's Algorithm)

Here, Public key PU(e, n)=7, 33
Private key PR(d, n)=3, 33
Suppose, the Plaintext value (M) is 5 then,

6. For Encryption,
   Ciphertext $C = M^e \bmod n$
   $= (5)^7 \bmod 33$
   $= 78125 \bmod 33$
   $= 14$

7. For Decryption,\
   Plaintext $P = C^d \bmod n$
   $= 11^3 \bmod 33$
   $= 2744 \bmod 33$
   $= 5$

Discrete Logarithm

It is easy to compute

$2^5 = 32$

But what about $3^i = 129140163$

It's not easy to compute the inverse of this function (need more time or sometimes difficult to compute).

We can rewrite the above power functions into logarithmic form.

$$5 = log_2(32)$$

$$i = log_3(129140163),$$

We can try to find $i = 17$. This type of function called one way function (easy in one direction but difficult reverse direction).

In general: $p^i = q$ can be written into $i = log_p(\mathrm{q})$, this for normal logarithm.

For logarithm with modular arithmetic become **Discrete logarithm.** Again we compute in modular arithmetic:

For **example:** $3^4 \bmod 12 = ?$

It's easy to find the results which is **9**, but what about this example

$$14^i \bmod 29867 = 26067$$

It's easy to compute the first one but difficult for the second one. We need to use try and error to find the value of $\boldsymbol{i}$, which is $\boldsymbol{i = 12}$ the correct one.

We can write the discrete logarithm in this form:

$$4 = dlog_{3,12}(9) \text{ and } 12 = dlog_{14,29867}(26067)$$

Discrete logarithm is one example of one way function (trap-door- function).

In general: $\boldsymbol{b = a^i \ (mod\ p)\ or\ i = dlog_{a,p}(b)}$

Example: Find $2^5 \ mod\ 3$ and $4^4 \bmod 11$

$$2^5 \bmod 3 = 32 \bmod 3 = 2$$

$$4^4 \bmod 11 = 256 \bmod 11 = 3$$

Example: Find the value of i for $8 = 5^i \bmod 13$

So the answer is $i = 3$

If we check: there are other values for $\boldsymbol{i}$:

$$8 = 5^7 \bmod 13$$

$$8 = 5^{11} \bmod 13$$

$5^0 \bmod 13$	1
$5^1 \bmod 13$	5
$5^2 \bmod 13$	12
$5^3 \bmod 13$	8

Both of them gives same results, so what is the exact value of $\boldsymbol{i = 3\ or\ 7\ or\ 11}$.

For cryptography we need unique value (distinct) for discrete logarithm. Therefore, we should consider cases only when $dlog$ gives us a unique answer.

$$b = a^i \ (\text{mod}\ p)\ or\ i = dlog_{a,p}(b)$$

We can get a unique value of i if a is a primitive root of prime modula p.

$$b = a^i \ (\text{mod}\ p)$$

Primitive root

Primitive Roots:

To understand primitive root let $p = 13$ based on discrete logarithm

$$b \equiv a^i (\text{mod } 13)$$

We need to find values of $\boldsymbol{a}$ to be a primitive **of** p

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	Distinct
1	1	1	1	1	1	1	1	1	1	1	1	1	X
2	2	4	8	3	6	12	11	9	5	10	7	1	✓
3	3	9	1	3	9	1	3	9	1	3	9	1	X
4	4	3	12	9	10	1	4	3	12	9	10	1	X
5	5	12	8	1	5	12	8	1	5	12	8	1	X
6	6	10	8	9	2	12	7	3	5	4	11	1	✓
7	7	10	5	9	11	12	6	3	8	4	2	1	✓
8	8	12	5	1	8	12	5	1	8	12	5	1	X
9	9	3	1	9	3	1	9	3	1	9	3	1	X
10	10	9	12	3	4	1	10	9	12	3	4	1	X
11	11	4	5	3	7	12	2	9	8	10	6	1	✓
12	12	1	12	1	12	1	12	1	12	1	12	1	X

Only (2, 6, 7 and 11) have distinct values (not repeated) and normally distributed from 1 to $(\boldsymbol{p-1})$ (12 in this example) so they are primitive roots of **13**. In other word, if we select $\boldsymbol{a}$ one of these values (2 or 6 or 7 or 11) then only one vales for $\boldsymbol{i}$ can satisfy the above discrete logarithm value.

Example: Check whether 2 is a primitive root of prime number 5?

2^1 mod 5	2 mod 5	2	✓
2^2 mod 5	4 mod 5	4	✓
2^3 mod 5	8 mod 5	3	✓
2^4 mod 5	16 mod 5	1	✓

Yes, **2** is a primitive root of prime number 5 because the numbers are distinct and consist of the integers from 1 through $(5-1)$ in some permutation.

Diffie-Hellman Key Exchange

Global Public Elements

p	prime number
a	$a < p$ and a a primitive root of p

User A Key Generation

Select private X_A	$X_A < p$
Calculate public Y_A	$Y_A = \alpha^{XA} \bmod p$

User B Key Generation

Select private X_B	$X_B < p$
Calculate public Y_B	$Y_B = \alpha^{XB} \bmod p$

Calculation of Secret Key by User A

$K = (Y_B)^{XA} \bmod p$

Calculation of Secret Key by User B

$K = (Y_A)^{XB} \bmod p$

Example: Let the key exchange is based on the use of the prime number $p = 7$.

Step 1: The prime number $p = 7$ and select a primitive root of $p = 7$ as $a = 5$ $(any\ no. a < p)$.

5^1 mod 7	5 mod 7	5	✓
5^2 mod 7	25 mod 7	4	✓
5^3 mod 7	125 mod 7	6	✓
5^4 mod 7	625 mod 7	2	✓
5^5 mod 7	3125 mod 7	3	✓
5^6 mod 7	15,625 mod 7	1	✓

Then $a = 5$ is the primitive root of $p = 7$

Step 2: We assume the private key for our sender as $X_A = 3$ where $X_A < 7$. The public key can be calculated as $Y_A = a^{X_A}\ mod\ p$.

$$Y_A = 5^3 \bmod 7 = 125 \bmod 7 = 6$$

So, the key pair for your sender becomes $\{X_A = 3, Y_A = 6\}$.

Assume the private key for the receiver to be $X_B = 4$ where$X_B < 7$. The public key for the receiver is calculated as $Y_B = a^{X_B} \bmod p$.

$$Y_B = 5^4 \bmod 7 = 625 \bmod 7 = 2$$

For the receiver, the key pair becomes $\{X_B = 4, Y_B = 2\}$.

Step 3: To generate the final secret key, for the sender, $K = (Y_B)^{X_A} \; mod \; p$.

$K = (2)^3 \bmod 7 = 8 \bmod 7$

$K = 1$

for the receiver $K_2 = (Y_A)^{X_B} \bmod p$

$K = (6)^4 \bmod 7 = 1296 \; mod \; 7$

$K = 1$

Both ***K*** are the same, the key exchange is success.