RSA example

Step 1: Let $p = 7$, $q = 11$

Step 2: $n = p * q = 7 \times 11 = 77$

Step 3: $\phi(n) = (p-1)(q-1) = 6 * 10 = 60$

Step 4: Let $e = 17$

Step 5: $d \equiv e^{-1} \bmod \phi(n)$

$de \bmod \phi(n) = 1$

$d * 17 \bmod 60 = 1$

Using Euclidean algo

$60x + 17y = 1$

$\therefore 60 = 3(17) + 9$

$17 = 1(9) + 8$

$9 = 1(8) + 1$

Then using extended Euclidean

$1 = 9 - 1(8)$

$1 = 9 - 1(17 - 1(9))$

$1 = 2(9) - 1(17)$

$1 = 2(60 - 3(17)) - 1(17)$

$1 = 2(60) - 6(17) - 1(17)$

$1 = 2(60) - 7(17)$

Here d is negative so subtract from 60.

$\therefore d = 60 - 7 = 53$

The public key = {17, 77}

private key = {53, 77}

Now for example plaintext is 8.

$\therefore C = 8^{17} \bmod 77$

$= (8^4 \bmod 77 \times 8^4 \bmod 77 \times$

$8^4 \bmod 77 \times 8^4 \bmod 77 \times$

$8 \bmod 77) \bmod 77$

$= (15 \times 15 \times 15 \times 15 \times 8) \bmod$

$= 57$

similarly for decryption

$57^{53} \bmod 77 = 8$

RSA

Example -(3)

(1) $p = 3$, $q = 11$

(2) $n = p * q = 33$

(3) $\phi(n) = (p-1) * (q-1) = (2)(10) = 20$

(4) Let $e = 7$

(5) Now $de \bmod \phi(n) = 1$

$d * 7 \bmod 20 = 1$

According to Euclidean

$$20 = 2(7) + 6$$
$$7 = 1(6) + 1$$

Now we take Extended Euclidean

$$1 = 7 - 1(6)$$
$$1 = 7 - 1(20 - 2(7))$$
$$1 = 7 - 1(20) + 2(7)$$
$$1 = 3(7) - 1(20)$$

$\therefore \boxed{d = 3}$

Here Public Key $= \{7, 33\}$

private key $= \{3, 33\}$

For plaintext = 5

$C = 5^7 \bmod 33$

$= (5^2 \bmod 33 \times 5^2 \bmod 33 \times 5^2 \bmod 33 \times 5 \bmod 33) \bmod 33$

$= (25 \times 25 \times 25 \times 5) \bmod 33$

$C = 14$

For decryption:

$P = C^d \bmod 33$

$= 14^3 \bmod 33$

$P = 5$

RSA example

1) $p = 5, q = 11$

2) $n = p * q = 5 * 11 = 55$

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

4) Now let $e = 3$

5) According to GCD

$$d e \bmod \phi(n) = 1$$

$$d * 3 \bmod 40 = 1$$

According to Euclidean algo

$$40 = 13(3) + 1$$

Now using back substitution

$$1 = 40 - 13(3)$$

Here $d = -13$ Therefore subtract from $\phi(n)$ we get $d = 40 - 13$

$$\boxed{d = 27}$$

(6) If plaintext = 9

$C = 9^3 \bmod 55$

$\boxed{C = 14}$

7) and Decryption

$P = 14^{27} \bmod 55$

$\boxed{P = 9}$

RSA example

(1) $p = 11$, $q = 13$

(2) $n = p * q = 13 * 11 = 143$

(3) $\phi(n) = (p-1) * (q-1) = 10 * 2 = 120$

(4) Now Let $e = 11$

(5) $de \bmod \phi(n) = 1$

$d * 11 \bmod 120 = 1$

According to Euclidean Algo

$120 = 10(11) + 10$

$11 = 1(10) + 1$

Now according to back substitution

$1 = 11 - 1(10)$

$1 = 11 - 1(120 - 10(11))$

$1 = 11(11) - 120(1) + 10(11)$

$1 = 11(11) - 120(1)$

Hence $d = 11$

Here public key = {11, 143}
private key = {11, 143}

(6) For plaintext = 7

$$C = 7^{11} \bmod 143$$

$$C = (7^4 \bmod 143 \times 7^4 \bmod 143 \times 7^2 \bmod 143 \times 7 \bmod 143)$$

$$\boxed{C = 106}$$

(7) For decryption

$$P = (106)^{11} \bmod 143$$

$$\boxed{P = 8}$$

RSA - Example - 6

1) $p = 17$, $q = 31$

2) $n = p * q = 17 * 31 = 527$

3) $\phi(n) = (p-1) * (q-1) = (16)(30)$

$\phi(n) = 480$

4) Let $e = 7$

5) $de \bmod \phi(n) = 1$

$7d \bmod 480 = 1$

According to Euclidean algo

$480 = 68(7) + 4$

$7 = 1(4) + 3$

$4 = 1(3) + 1$

Now according to Back substitution

$1 = 4 - 1(3)$

$1 = 4 - 1(7 - 1(4))$

$1 = 4 - 1(7) + 1(4)$

$1 = 2(4) - 1(7)$

$1 = 2(480 - 68(7)) - 1(7)$

Page
Date

$1 = z(480) - 137(7)$

480

Hence we get $d = \text{[illegible]} - 137$

$\boxed{d = 343}$

→ Here public key = {7, 527}

private key = {343, 527}

(b) If plaintext = 2

$\boxed{2^7 \bmod 527 = 128}$

Ciphertext

* DIFFIE - HELLMAN KEY EXCHANGE

→ The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

→ The algorithm itself is limited to the exchange of secret values.

Algorithm:

(User A) (User B)

Step 1: Sender and Receiver agree to select

q = prime number

α = $\alpha < q$ and α is primitive root of q

Step 2: User-A selects private key "a" such that $a < q$.

→ User-B selects private key "b" such that $b < q$.

Step 3: User-A Calculates public key.

$$Y = \alpha^a \bmod q$$

Page
Date

Step-4: User - B calculates public key

$$X = \alpha^b \bmod q$$

Step 5: User - A sends his public key 'Y' to User - B and User - B sends his public key 'X' to User - A.

Step 6: User - A calculates the secret key

$$K = (X)^a \bmod q$$

Step 7: User - B calculates the secret key

$$K = (Y)^b \bmod q$$

→ As a result the two sides have exchanged a secret value.

→ This whole concept is based on discrete Logarithm.

→ Thus while it is relatively easy to calculate exponentials modulo a prime, it is very d to calculate discrete logarithms

* Extra knowledge for understanding Diffie Hellman

-> What is primitive roots?

Ans If the prime number is p, a primitive root (or generator) g is a number, that when n goes from 1 to p-1,

then $g^n \bmod p$ goes through all the numbers $1 \ldots (p-1)$ in some order.

-> $g^n \bmod p$ means the remainder when you raise g to n and divide by p.

-> Example:

Let's show that 3 is one of the primitive roots of prime number 5 but 4 is not.

-> 3 is a primitive root of 5:

n	3^n	$3^n \bmod 5$
1	3	3
2	9	4
3	27	2
4	81	1

→ Here we take all the integers starting with 1, right upto one less than 5 in 1st

→ Then we raise our candidate root 3 to each number, generating the sequence of powers in the second column.

→ We divide the result by our prime 5 and record the remainders in third column.

→ If the set of remainders in the third column reproduces the set of integers in the first (order need not be identical), then 3 is the primitive root.

→ From above discussion we can say that 3 is indeed a primitive root of 5.

4 is not a primitive root of 5:

x	x^x	$x^x \bmod 5$
1	4	4
2	16	1
3	64	4
4	256	1

→ Here the set of integers in first and third column is not same. So 4 is not a prime root of 5.

Example-1 of Diffie Hellman.

Step 1: $q = 13$

$\alpha = 6$

Step 2: User-A secret key $a = 3$

User-B secret key $b = 10$

Step 3: User - A calculates public key

$$Y = 6^3 \bmod 13$$

$$Y = 8$$

Step 4: User - B calculates public key

$$X = 6^{10} \bmod 13$$

$$X = 4$$

Page
Date

Step 5: User - A gets $x = 4$ and User - B get $y = 8$

Step 6: Secret key calculated by User-A

$$K = (x)^a \bmod q$$

$$= 4^3 \bmod 13$$

$$\boxed{K = 12}$$

Step 7: Secret key calculated by User - B

$$K = (y)^b \bmod q$$

$$K = 8^{10} \bmod 13$$

$$\boxed{K = 12}$$

Example-2 Diffie Hellman

Step 1) $q = 23$ $\alpha = 5$ (primitive root of 23)

Step 2) User-A chooses private key

$a = 6$

User-B chooses private key

$b = 15$

Step 3: User-A calculates public key

$$y = 5^{6} \bmod 23$$

$$\boxed{y = 8}$$

Step 4: User-B calculates public key

$$X = 5^{15} \bmod 23$$

$$\boxed{X = 19}$$

Step 5: User-A calculates secret key

$$K = 19^{6} \bmod 23 = 2$$

Step 6: User-B calculates secret key $K = 8^{15} \bmod 23 = 2$

* Man-in-the-middle Attack

-> Diffie Hellman is insecure against a man-in-the middle attack.

-> Suppose Alice and Bob wish to exchange keys, and Darth is the attacker.

Step 1: Darth prepares for the attack by generating two random private keys

D_1 and D_2.

Step 2: Darth computes corresponding public keys

$$Y_{D_1} = \alpha^{D_1} \bmod q$$

$$Y_{D_2} = \alpha^{D_2} \bmod q$$

Step 3: Alice transmits its public key Y to Bob by computing $Y = \alpha^b \bmod q$

Step 4: Darth intercepts Y and transmits Y_{D_1} to Bob. Darth calculates $K_2 = (Y)^{D_2} \bmod q$

Steps: Bob receives Y_{D1} and calculates

$$K_1 = (Y_{D1})^b \bmod q$$

Step6: Bob transmits X to Alice

Step7: Darth intercepts X and transmits Y_{D2} to Alice

Darth calculates $K_1 = (X)^{D1} \bmod q$.

Step8: Alice receives Y_{D2} and calculates

$$K_2 = (Y_{D2})^a \bmod q$$

→ At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key K_1 and Alice and Darth share secret key K_2.

→ All future communication between Bob and Alice is compromised.

Page
Date

Some important Theories:

(1) **Diffusion Vs. Confusion**

→ A ciphertext has the possibility of being broken by using statistical analysis that can provide some information on frequency of characters which can then be compared to a known language.

→ For example, the letter 'e' has the highest usage in English language and therefore a cryptanalyst may match the highest frequency of a character in the ciphertext to letter 'e'.

→ For a ciphertext to be secure enough, it is important that statistical or frequency analysis on the ciphertext would not yield enough information to break it.

→ This is possible by providing "**Confusion**" and "**Diffusion**" through encryption process.

→ **Confusion** : It means that the key does not relate in a simple way to the ciphertext.

→ Each character of the ciphertext should depend on several parts of the key.

→ This makes relationship between ciphertext and key as complex as possible.

Example : In stream cipher 'one-time pad' is the example of Confusion.

→ S-boxes in DES and AES are examples of confusion.

(2) Diffusion : To make it hard for the statistical attacks, the cryptographer could dissipate the statistical structure of the plaintext in the long range statistics of the ciphertext.

→ This process is called as diffusion.

→ This is possible if many of the plaintext characters can affect each of the ciphertext characters.

→ When such a process takes place, the ciphertext characters will no longer have matching characters in plaintext in terms of statistics.

→ Example : Permutation in DES and AES