Semester : VI Subject : CSS Academic Year: 2023 - 2024

RSA Algorithm:

There are 3 steps in RSA Algorithm:

- * Key generation.
- * Encryption
- * Decryption.

Key Generation:

* Select p, q.	p, q should be a prime number.
* Calculate n.	$n = p * q$.
* Calculate $\phi(n)$	$\phi(n) = (p-1)(q-1)$.
* Select integer e	$\gcd(\phi(n), e) = 1, e < \phi(n)$.
* Calculate d	$d = \frac{k\phi(n)+1}{e}$
Public key of Receiver.	$K_u = \{e, n\}$
Private key of Receiver	$K_R = \{d, n\}$.

Encryption:

Plain Text.	M.
	$M < n$.
Calculate Cipher Text.	$\boxed{C = M^e \bmod n}$

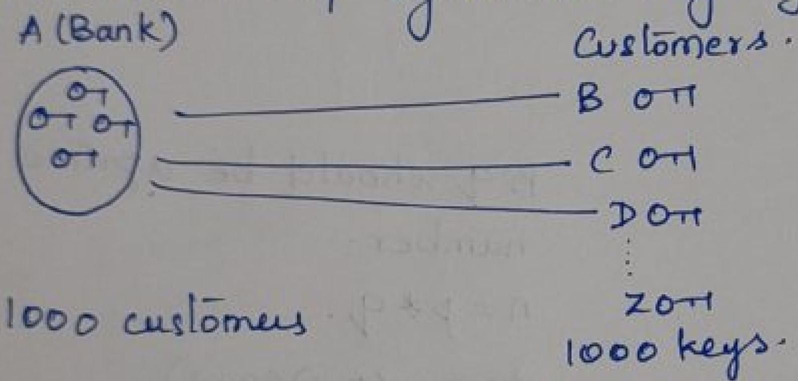
Decryption:

Cipher Text.	C.
Plain Text.	$\boxed{M = C^d \bmod n}$.

Semester : VI Subject : CSS Academic Year: 2023- 2024

RSA Algorithm:

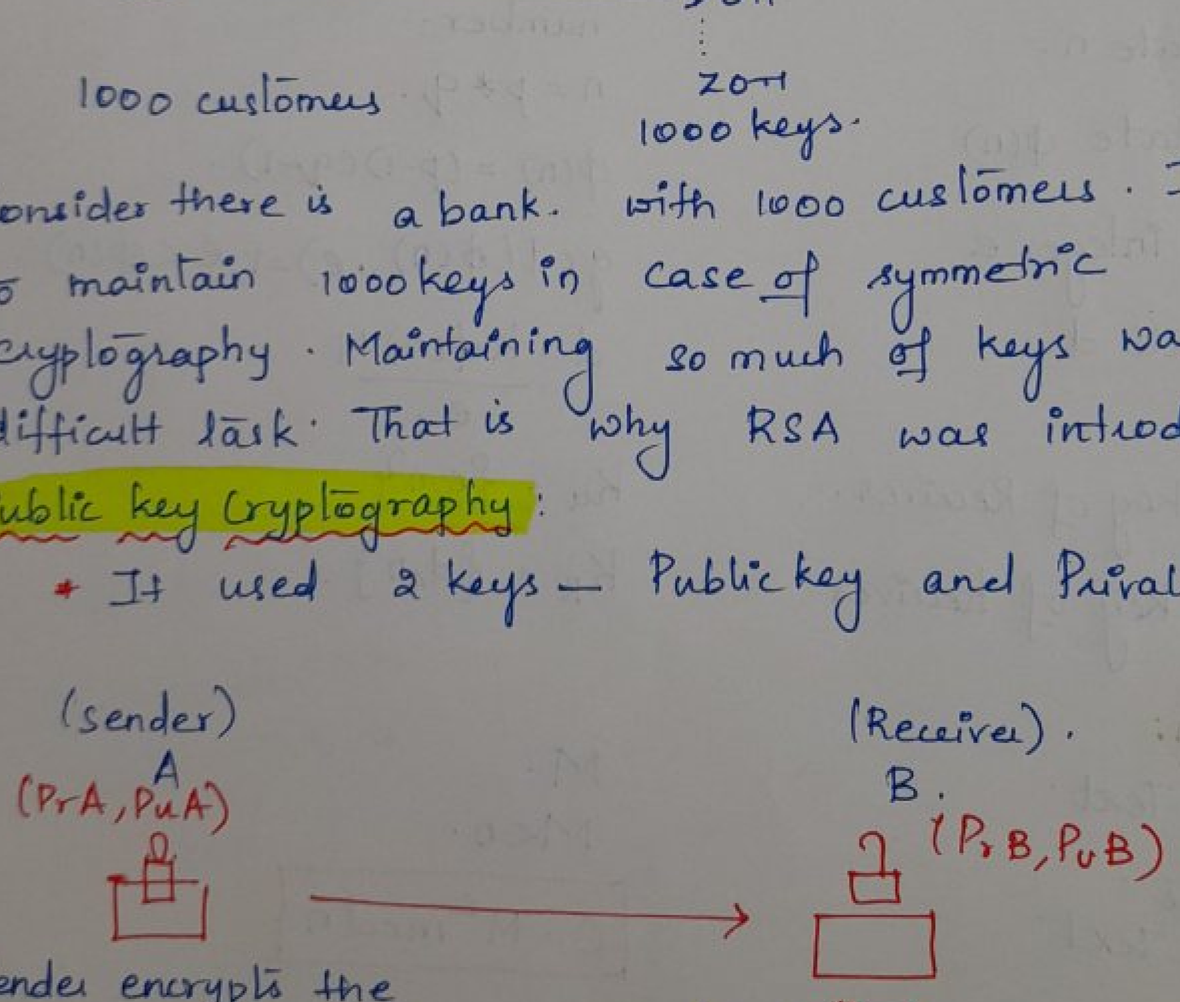
* It was invented in the year 1977 by Rivert, Shamir and Adleman.
* RSA uses the concept of public key cryptography.
* The drawback of symmetric key Cryptography:



Consider there is a bank with 1000 customers. It has to maintain 1000 keys in case of symmetric cryptography. Maintaining so much of keys was a difficult task. That is why RSA was introduced.

Public key Cryptography:

* It used 2 keys – Public key and Private key.



Sender encrypts the message using PuB. (Public key of Receiver).

Receiver decrypts the message using his own private key (PrB).

Example 1:

Consider the sender has to send message M=10, Given p1=7 and p2=17.

(i) Calculate e and d

(ii) Find the Cipher Text by encryptiong with public key.

(iii) Find the plain Text by decypting with private key.

Given: $p_1 = 7,\ p_2 = 17.$

$n = 7 * 17 = 119$

$\boxed{n = 119}$

$\phi(n) = (p_1 - 1)(p_2 - 1)$

$= (6)(16)$

$\boxed{\phi(n) = 96}$

$$\begin{array}{r|l} 2 & 96 \\ \hline 2 & 48 \\ \hline 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline 3 & 3 \\ \hline & 1. \end{array}$$

Select e,

$96 = 2 \times 2 \times 2 \times 2 \times 2 \times 3.$

$\boxed{e = 5}$

Calculate d:

$d = \frac{k(\phi(n)) + 1}{e}$

$= \frac{k \times 96 + 1}{5} = \frac{4 \times 96 + 1}{5}$

[In this case k should be 4 so that we get whole number as output].

$= \frac{384+1}{5} = \frac{385}{5}$.

$\boxed{d = 77}$

Encyption :

$C = M^e \bmod n$.

$= 10^5 \bmod 119$.

$= 100000 \bmod 119$.

How to calculate modulus manually.

100000 % 119.

(1) Start by choosing the initial number : 100000.

(2) Choose the divisor : 119.

(3) Divide one number by another, rounding down :

$100000 / 119 = 840$.

(4) Multiply the divisor by the quotient.

~~10 * 24 = 240~~. 840 * 119 = 99,960

(5) Subtract this number from your initial number.

~~250~~- . 100000 − 99960 = 40.

(6) The number obtained is the result of modulus operation.

$\boxed{C = 40}$

$M = C^d \bmod n$

$= 40^{77} \bmod 119$.

The method to calculate when huge values are given:

	64	32	16	8	4	2	1
77 =	1	0	0	1	1	0	1

$40^{77} = 40^{64} \cdot 40^{8} \cdot 40^{4} \cdot 40^{1}$ [wherever 1 is there, we consider that].

$(a \times b) \bmod n = (a \bmod n \times b \bmod n) \bmod n$.

$\boxed{40^1 \bmod 119 = 40}$

$40^2 \bmod 119 = (40 \times 40) \bmod 119$.

$= (40 \bmod 119)\ (40 \bmod 119) \bmod 119$

$= (40)(40) \bmod 119$

$= 1600 \bmod 119$.

$\boxed{40^2 \bmod 119 = 53}$.

$40^4 \bmod 119 = (40^2 \times 40^2) \bmod 119$

$= (40^2 \bmod 119)\ (40^2 \bmod 119)$.

$= (53)\ (53) \bmod 119$.

$= 2809 \bmod 119$.

$\boxed{40^4 \bmod 119 = 72}$.

Semester : VI Subject : CSS Academic Year: 2023-2024.

$40^{8} \bmod 119 = (72)(72) \bmod 119.$

$= 5184 \bmod 119.$

$\boxed{40^{8} \bmod 119 = 57.}$

$40^{16} \bmod 119 = (67)(67) \bmod 119$

$= 4489 \bmod 119.$

$\boxed{= 86}.$

$40^{32} \bmod 119 = (86)(86) \bmod 119.$

$= 7396 \bmod 119$

$\boxed{= 18.}$

$40^{64} \bmod 119 = (18)(18) \bmod 119.$

$= 324 \bmod 119.$

$\boxed{= 86}.$

$40^{77} = 40^{64} . 40^{8} . 40^{4} . 40 \bmod n.$

$= (86).(67).(72).(40) \bmod 119.$

$\boxed{M = 10}.$

Semester : VI Subject : CSS Academic Year: 2023- 2024

Example : 2

Given values $p_1 = 11$, $p_2 = 13$ and plain Text $M = 9$.

(i) Find the encryption and decryption keys.

(2) Calculate the Cipher Text.

Solution :

Given $p1 = 11$, $p2 = 13$.

$n = p1 * p2$

$= 11 * 13$

$\boxed{n = 143}$

$$\begin{array}{r|l} 2 & 120 \\ 2 & 60 \\ 2 & 30 \\ 3 & 15 \\ & 5 \end{array}$$

$\phi(n) = (p_1 - 1) * (p_2 - 1)$

$= (10) * (12)$

$\boxed{= 120}$

Select e,

$120 = 2 \times 2 \times 2 \times 3 \times 5$

$\boxed{e = 7.}$

$d = \frac{k \cdot \phi(n) + 1)}{e.}$ $(k = 6)$.

$= \frac{6 \times 120 + 1}{7}$ $\boxed{d = 103.}$

$C = M^e \bmod n.$

$= 9^7 \bmod n.$

$= 4782969 \bmod 143$ $\boxed{= 48.}$

$M = C^{d} \bmod N$

$= 48^{103} \bmod 143$.

$\boxed{M = 9}$.

Example 3:

The Given values are p1 = 53, P2 = 59 and M = 89 .
Calculate e, d and Cipher Text.

Solution:

Given $p_1 = 53$, $p_2 = 59$

$n = p_1 * p_2$.

$= 53 * 59$

$\boxed{n = 3127}$

$\phi(n) = (p_1 - 1)(9p_2 - 1)$

$= (52)(58) = 3016$.

$\boxed{\phi(n) = 3016}$

2 | 3016
2 | 1508
2 | 754
377

Select e,

In this case $\boxed{e = 3.}$

$d = \frac{k \cdot \phi(n) + 1}{e}$ (k = 2) .

$= \frac{2 * 3016 + 1}{3} = 2011$

$\boxed{d = 2011}$

$C = M^e \bmod n$

$= 89^3 \bmod 3016.$

$\boxed{C = 1394}$

$M = C^d \bmod n.$

$= 1394^{2011} \bmod 8127.$

$\boxed{M = 89}$