

IT 653 Network Security
Assignment 1

Submitted by Ramrao Wagh
Roll number 03429801

Performance Analysis of RSA Algorithm

1. The First Study was made on the time taken to generate the public key, encryption time and decryption time on the same message by varying the key size.

The same program was executed five times to account for variations.
The file containing the output of these five runs is attached as rsatimedatasamples.txt
A output of one such run is shown here:
Run 2

KeySize	Key Generation Time	Encryption Time	Decryption Time	Total
Time in ms				
128	125	78	94	297
256	94	562	594	1250
512	781	3922	3953	8656
768	1110	12750	12625	26485
1024	15312	29235	29437	73984

The following observations are made:

1. Key generation time increases rapidly with increase in key size, however usually a drop in key generation time is seen for keysize 256 bits.
2. Encryption and Decryption times also increase very fast with increase in key size
3. Both, the encryption and decryption time increase in same amount over key size increase
4. The total time taken to perform all these operations changes with change in key generation time.

2. The second study was made by changing the message size and running the algorithm by specifying two key sizes.

The size of the message was varied from 0, 1, 2, 3,& 4KB and the key size of 512 & 1024 was applied for each message input.

a sample run is shown as below:

Message Size: 0 KB

Keysize Time in ms	Key Generation Time	Encryption Time	Decryption Time	Total
512	969	0	0	969
1024	12141	0	0	12141

Message Size : 1 KB

512	390	9750	9656	19796
1024	9657	69281	69109	148047

Message Size: 2 KB

512	328	18359	18422	37109
1024	7047	140985	137156	285188

Message Size: 3 KB

512	594	27640	27969	56203
1024	1062	215906	212282	429250

Message Size: 4 KB

512	578	37015	37547	75140
1024	19625	274141	274015	567781

1. It is seen that Encryption time and Decryption time increase dramatically with increase in message size.

3. The Third study was made by running the same program and input that was used for study 1 but by changing the probability value for generation of p & q being prime in the BigInteger constructor

The following table was constructed from the output of the program:

Size	<-----			probability ----->			
	5	10	20	30	40	50	100
128	109	140	125	125	219	125	297
256	610	140	390	140	562	203	515
512	360	344	314	1000	1015	531	531
768	2344	2828	1907	2828	938	1797	813
1024	8968	3438	5625	8266	8563	4859	9453

The cells in the matrix denote the time for key generation of the size shown in the row when the certainty value was changed as shown in column headings from 5 to 100.

It is observed that there is a slow rise in general in key generation as the certainty value is increased but it is not conclusive, as the values do not show any particular pattern. The fluctuation in key generation time is more for higher Key size.

Graphs based on the data collected are enclosed herewith for reference.