IT 653: Network Security
Assignment 1 - Part 2
Study of the time complexity of RSA algorithm

Shweta Agrawal

August 16, 2003

1 For different key sizes

The various input parameters were as follows:

- key size: varied from 128 byte to 1024 byte with an interval of 128.
- message size: about 1 KB.
- certainity value: fixed to 10. (probability of P, Q being prime $\geq 1 - 1/2^{certainity}$)

Resulting graph

Analysis: The encryption and decryption times increase exponentially as can be seen in the graph. The explanation for this is the formula for encryption and decryption which is exponential in key.

$$Encryption : C = M^e mod n$$

$$Decryption : M = C^d mod n$$

where e and d are the public and private keys respectively. Thus the time for encryption and decryption are exponential function of key size. This key size is in turn directly determined by the size of the prime numbers P and Q chosen. Similarly the key generation time also increases exponentially as shown in a sepearate graph for clarity. This is due time to select two prime numbers by the algorithm (e.g. Miller Rabin algorithm) is exponential in terms of size of space available to search for it.

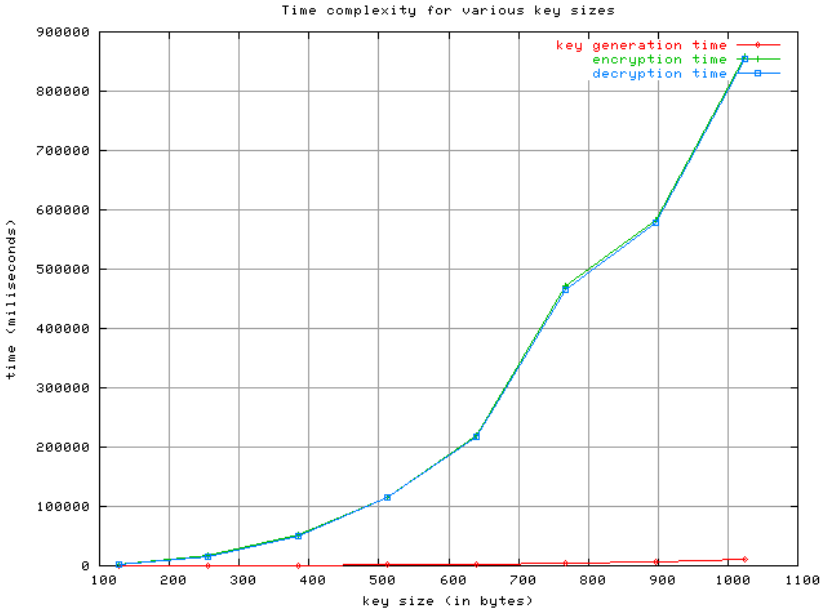

Figure 1: Key generation and Encryption/Decryption time

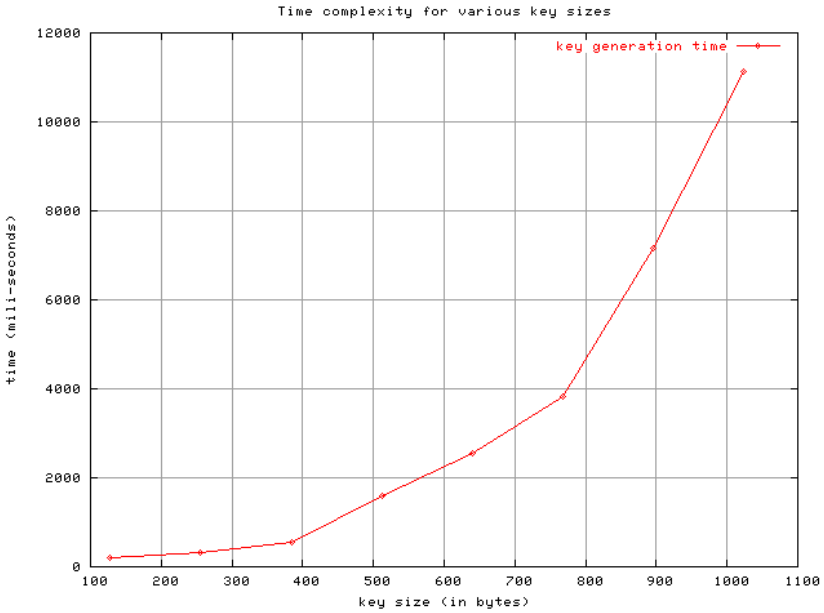

Figure 2: Key generation time

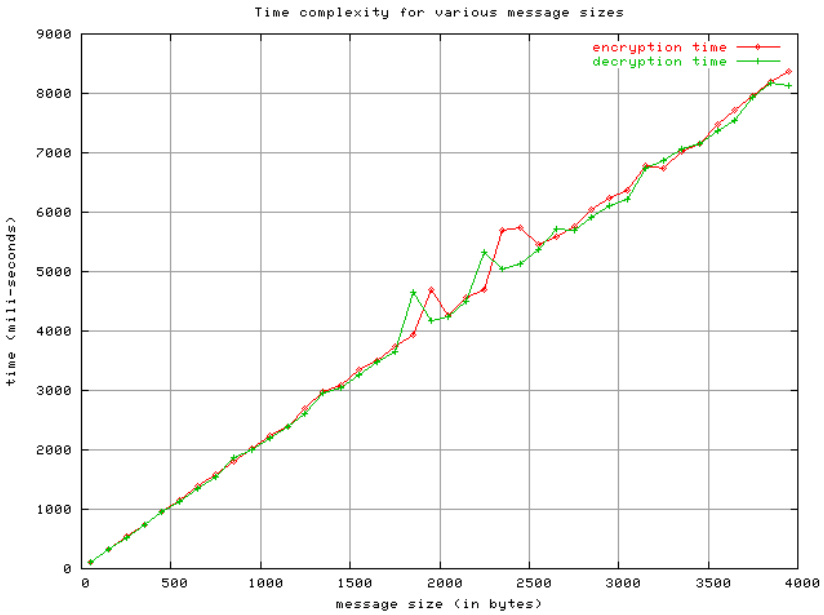

Figure 3: Encryption/decryption time for 128 byte keysize

2 For different message sizes

The various input parameters were as follows:

- key size: 128 and 256 bytes.
- message size: varying from 50 to 4000 bytes at an interval of 100.
- certainity value: fixed to 10. (probability of P, Q being prime $\geq 1 - 1/2^{certainity}$)

Resulting graph

Analysis: The encryption and decryption times increase linearly with the message size. The explanation for this is again the formula for encryption and decryption which is nearly linear in message.

3 For different values of certainity

The various input parameters

- key size: 256 bytes.
- message size: fixed message of about 1 KB in size.

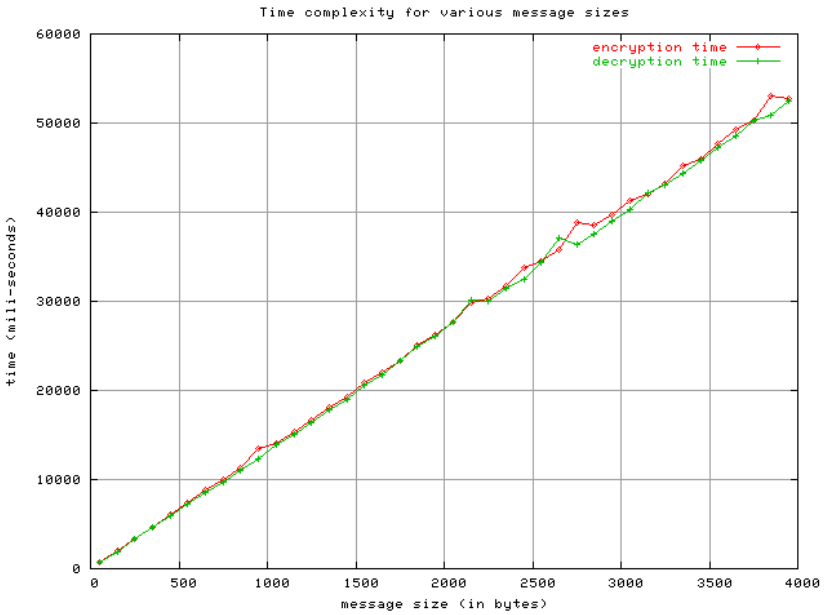

Figure 4: Encryption/decryption time for 256 byte keysize

- certainity value: probability of P, Q being prime $\geq 1 - 1/2^{certainity}$ varied from 1 to 50 with an interval of 2.

Result graph

Analysis Though, no clear pattern is seen in variation of time for generating a key pair for various values of certainity. The time generally increases with the increase in certainity, if we ignore some outliers in between.

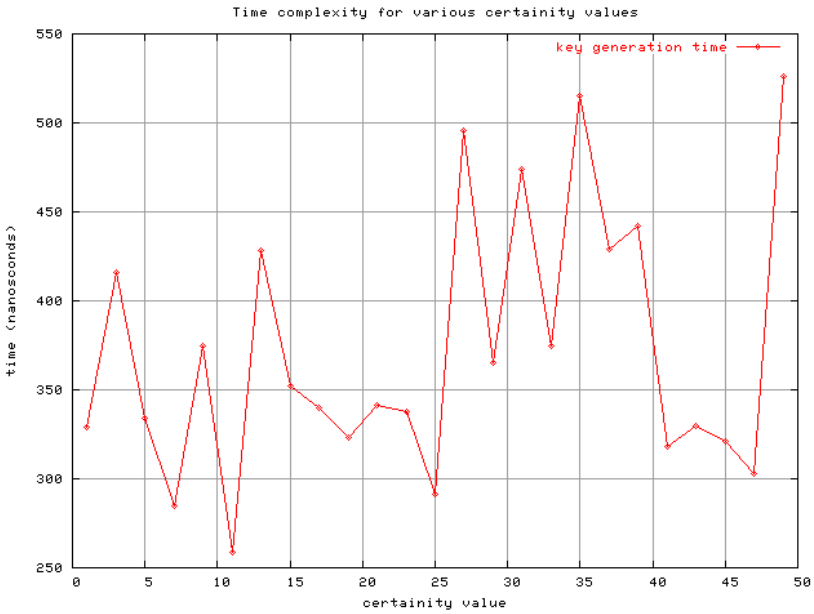

Figure 5: Key generation time