**RSA Assignment**

**Name:** Hoda Gamal Hamouda Ismail

**Code:** 9203673

**Section:** 2

**BN:** 34

**Efficiency Analysis:**

|  |  |
| --- | --- |
| Size of n (bits) | Time of encryption (seconds) |
| 28 |  |
| 32 |  |
| 64 |  |
| 128 |  |
| 256 |  |
| 512 |  |
| 1024 |  |

|  |  |
| --- | --- |
| Size of n (bits) | Time of decryption (seconds) |
| 28 |  |
| 32 |  |
| 64 |  |
| 128 |  |
| 256 |  |
| 512 |  |
| 1024 |  |

Comment:

Time of encryption/decryption increases exponentially with increasing of size of n, but it is still a short time, which makes the algorithm efficient in encryption/decryption.

**Attack Analysis:**

Chart

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
|  | Time of factorizing n (seconds) | Size of n (bits) | Time of factorizing n (seconds) |
| 27 |  | 46 |  |
| 28 |  | 47 |  |
| 29 |  | 48 |  |
| 30 |  | 49 |  |
| 31 |  | 50 |  |
| 32 |  | 51 |  |
| 33 |  | 52 |  |
| 34 |  | 53 |  |
| 35 |  | 54 |  |
| 36 |  | 55 |  |
| 37 |  | 56 |  |
| 38 |  | 57 |  |
| 39 |  | 58 |  |
| 40 |  | 59 |  |
| 41 |  | 60 |  |
| 42 |  | 61 |  |
| 43 |  | 62 |  |
| 44 |  | 63 |  |
| 45 |  | 64 |  |

Comment:

Time of factorizing n and get d increases exponentially with increasing of size of n.

Sizes until …..., can be broken at some seconds.

But from ……, it takes minutes to hours to get broken.

Which shows us how much RSA algorithm is secure.

And keys of large size such as 512 or 1024 are secure enough to use if the message will not be useful after days.