Cryptography Project  
  
Detailed Report

**Name Section Bench No.**

Essam Wisam 2 1

Mohamed Saad 2 14

Supervised by

Dr. Samir Shaheen

Eng. Sandra Wahid

May 2022

Table of Contents

[Implementation Details](#_dpv7yjpi1f2n) 3

[RSA Algorithm](#_w4gfnk9ztf7r) 3

[RSA World: End-to-end Encrypted Chat](#_ljfswfjkz4p6) 4

[RSA Encryption Efficiency Test](#_tf7xorchoixg) 5

[RSA Mathematical Brute-force Attack Test](#_ex8t62c7m5f8) 5

[RSA Chosen Ciphertext Attack](#_cv0kx6mp7teo) 7

[**Analysis Results & Conclusions**](#_bzzjjijdrw7o)7

[RSA Encryption Efficiency](#_801bun10givx) 8

[RSA Mathematical Brute-force Attack](#_qahwlbl1mor9) 9

[RSA Chosen Ciphertext Attack](#_1vqz42veuzkq) 11

[**Further Notes**](#_vkgnnaynensf)11

## Implementation Details

### RSA Algorithm

### Our implementation of the RSA algorithm is divided into two main parts. First, key generation where the user is assigned a private and public key: After providing their name, the user is free to either let their public and private keys be automatically generated; in which case we use Fermat’s test to generate two equally-sized large primes and then choose suitable such that where . We use the standard Euclidean algorithm to calculate the greatest common divisor and use the extended version to calculate the modular inverse which is used to calculate the private key as .

As for Fermat’s test which we use to generate primes, the number is surely composite if Fermat’s little theorem

does not hold, because it’s only guaranteed to work for prime numbers. Note that if it holds then we can’t say that the number must be prime (since some composite number can satisfy it as well) we get around the issue by applying the test many times while using different values of . We have learnt about this prime generation method in our number theory course.

The second main part of the RSA algorithm is encryption and decryption. Since it holds that

By Euclid’s Theorem (Provided ) then it also holds that

And because we generated keys such that

Then it’s true that

And hence

Which provided that yields

Thus, we implement encryption as

And decryption as

Clearly both of them boil down to simply implementing modular exponentiation. For that we used the binary exponentiation method presented in our book:

The only part that we didn’t explain so far is how our implementation of RSA is not just restricted to numbers. Our approach simply envisages in converting every character in the input string to its corresponding ASCII value. In more detail, //talk about the conversion

An additional note about encryption is that for the case where we will truncate the message to block of size smaller than and we could determine the maximum size as follows:

* + 1. Let a message consist of characters and each character is an 8-bit binary number, thus m as a number is less than or equals to .
    2. Using the above equation, the maximum message size n can hold could be deduced as follows thus thus could decrypt character in one go (the floor function is used as we only deal with integers).
    3. We truncate to messages each one contains at most characters and decrypt each one separately and send it.

The following table shows a list for some of the possible key generation input scenarios and our system’s response to them:

|  |  |
| --- | --- |
| Input | Response |
| Missing Name | Pop up message asking for the name. |
| Even e | Not Accepted regardless to p and q. |
| e that isn’t coprime with | Not accepted. |
| Any of p or q or e missing | Generate the missing values such that sign up is successful. |
| p and q that are not primes | Not accepted. |
| p and q of equal values | Not accepted since a single square root can break the cipher in this case. |
| Any of p or q or e not a number | The input values should be numbers. |
| p or q equals to 2 | The value of p and q must be greater than 2 (if p or q equals to 2 the keys are easily obtained). |
| e equals to 1 | The value of e should be greater than 1 (plain text would be send). |

### RSA World: End-to-end Encrypted Chat

We have used a text files approach where there is a main folder in which all user folders are contained and inside each user folder a text file is created that behaves like a receiving buffer that will be polled to know if a message was sent and decipher it. The first line of that file contains the public key of the user so as to if another user wants to communicate with him/her knows the public key to use in encryption.

**Initialization:**

The script gets the username and keys as a command line arguments and check if there is no user with that name exists if so, create its folder and text file.

**User selection**:

A window will appear to the user that lets the user see the available user and chose one on to chat with.

**Sending and Receiving**:

There are two separate threads for each one the receiving one poll the text file in the user folder if any message is found it decrypts it with the user private key and show the result in the window, the sending one check if the user enters a text on the window if so, it encrypts it with the public key of the other user that was obtained from the beginning of its file.

### RSA Encryption Efficiency Test

### // Write your implementation of the test here (that you prepare a numpy array of public keys, try to encrypt with each, what message did you use (it should be fixed), what e did you use (should be fixed as well I think,…)

### RSA Mathematical Brute-force Attack Test

### In the brute-force attack we try to factorize a set of public keys ranging from 8 to 1024 bit (8, 10, 12, …, 1024) and measure the time in each case. We used a very straightforward algorithm for integer factorization that simply searched for divisors of the given integer by considering those odd ones lying only in the range up till the integer’s square root. Once a divisor is found it’s guaranteed to be prime (because we are iterating from small numbers to larger ones) and dividing the public key by that should yield the other prime.

Note that however, as seen in the recursive algorithm below we keep looking for primes if after dividing the remaining number is composite and then report that the key isn’t due to RSA in a wrapper function if more than two primes are found.

def factorize(n):

if (n % 2) == 0:

return [2] + factorize(n//2)

integer = 3

while integer <= (n\*\*0.5):

if n % integer == 0:

return [integer] + factorize(n // integer)

else:

integer += 2 # Since all primes are odd.

return [n]

### RSA Chosen Ciphertext Attack

## In the chosen-cipher text attack we take as an input and of the victim along with a boolean “permission” that gives authority of their use to decrypt some chosen ciphertext. We also take the ciphertext that the attack is targeting (the one for which the attacker wants to know the corresponding ciphertext.) Within the algorithm we as well automatically generate the attack’s parameter r.

## The main modules are the Choose\_Y function which returns the chosen ciphertext by the attacker based on the target ciphertext, the attack parameter and victim’s public key.

## After Choosing the ciphertext we see if there is permission to decrypt it and if there is we use the result to get the corresponding message M to the target ciphertext.

def CCA(p, q, e, C, r, permission=True):

\_, \_, \_, \_, n, \_, d, err\_msg = sign\_up(str(p), str(q), str(e))

if err\_msg == '':

if GCD(r, n) != 1:

return "Could not establish the attack due to choice of r", -1

Y = Choose\_Y(C, r, n, e)

if permission:

X = ModExp(Y, d, n)

M = Find\_M(X, r, n)

return "", M

else:

return "Target denied signing.", -2

else:

return err\_msg, -3

Why does the attack happen?

The attack is possible due to the fact

Which follows as

And can be rephrased into

In the attack we let be the message we seek to read. From the communication channel we get

We then let be some integer such that and because we know our victim’s public key we compute

And then we either assume permission from the receiver to sign that (decrypt) or access to decryption device which because

Yields

And since we guaranteed earlier that , the attack is concluded since

This is, in-depth is all the math that makes the chosen-ciphertext attack possible.

Note that after all, it’s a chosen-ciphertext attack and some sort of access to the decryption device is needed. The common scheme for this is to ask the receiver to sign the chosen ciphertext (which is equivalent to decrypting it.)

## Analysis Results & Conclusions

### RSA Encryption Efficiency

In that we tried to encrypt a message with different key size starting from 8 to 1400 bits, and those are the results:

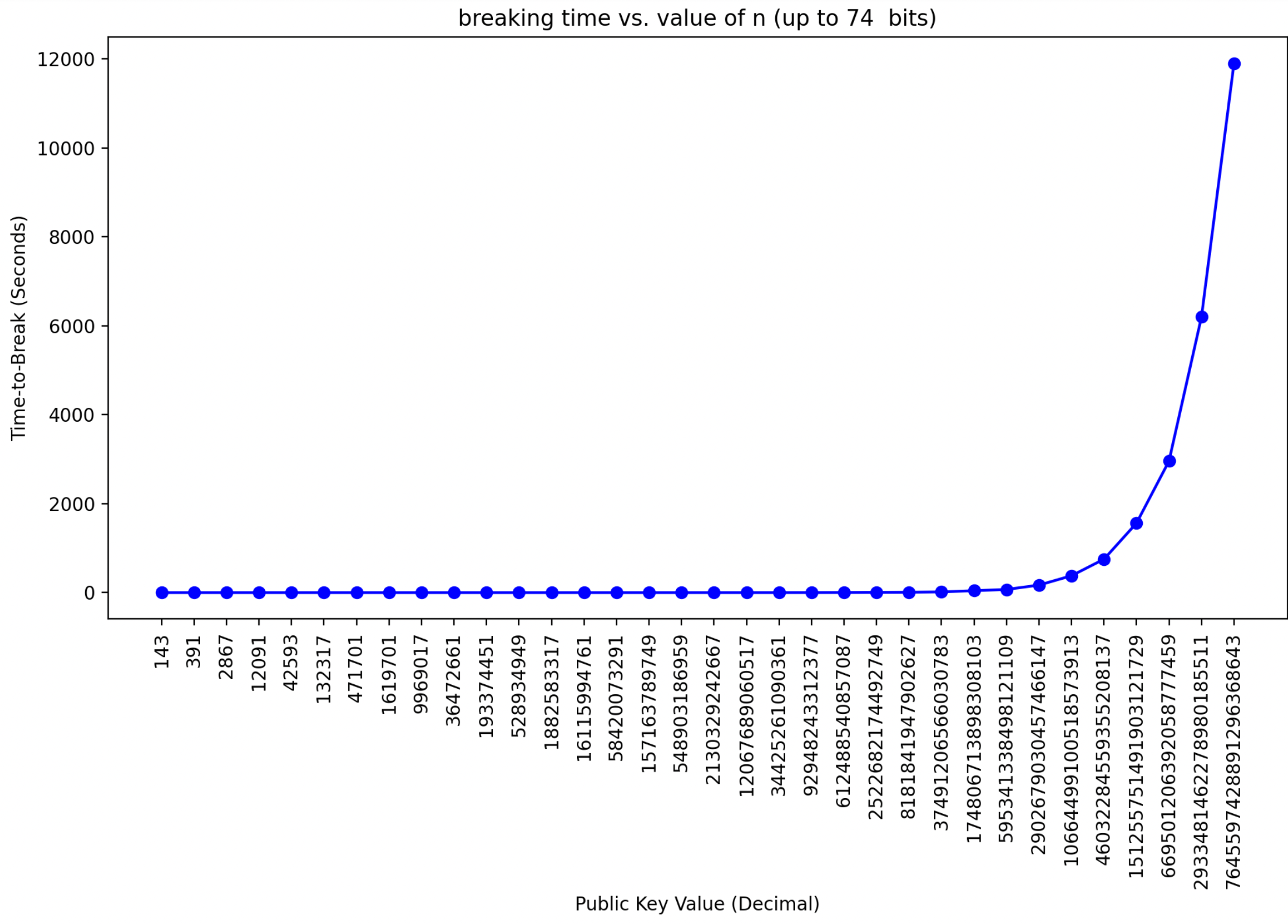
Chart, line chart

Description automatically generated

As we can see the encryption time goes in an exponential trend with the increase in size of n.

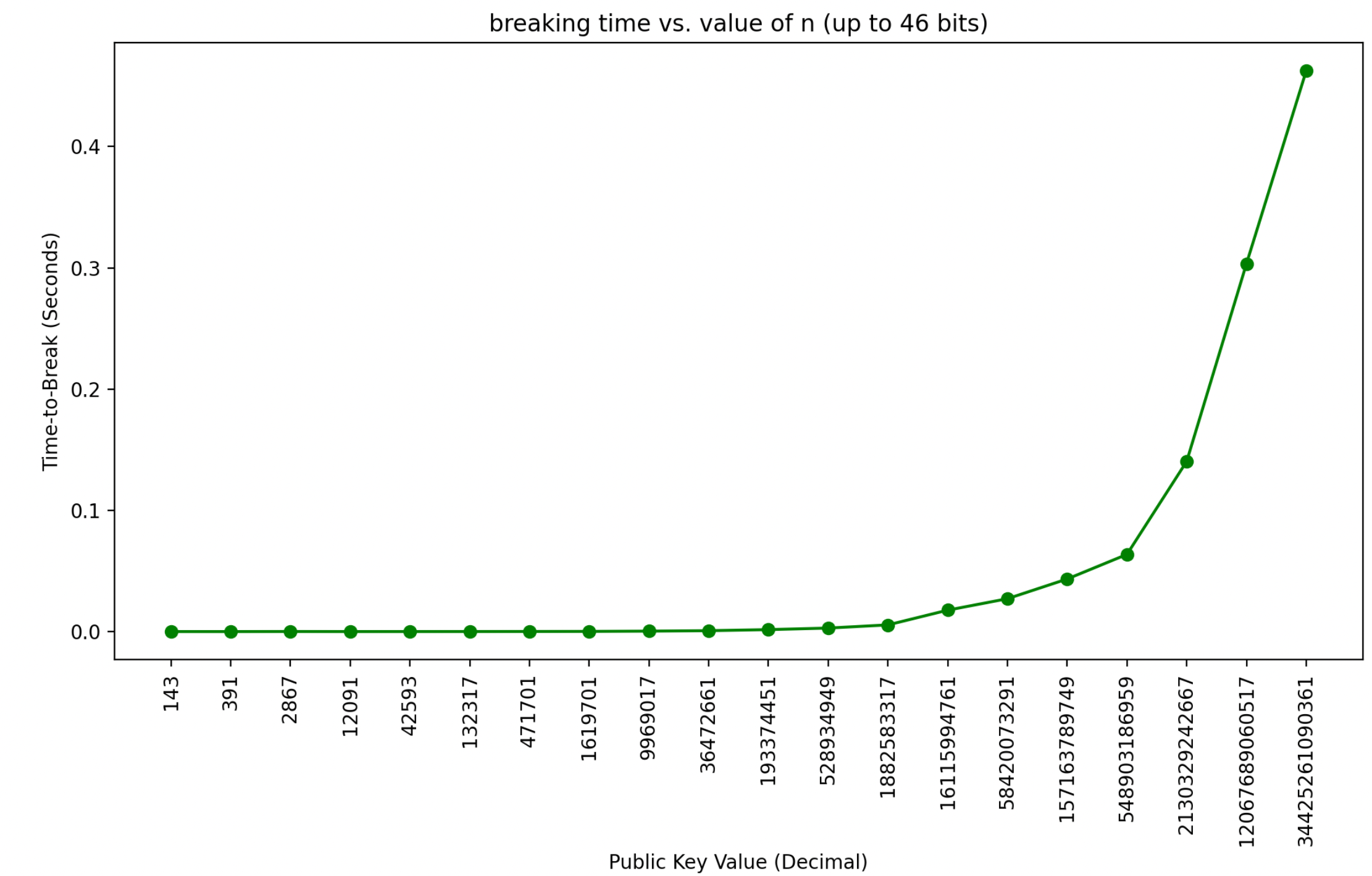
### // Write how much time did the whole thing take, how much time did the largest PU take what are the conclusions (e.g. affecting the choice of e). Write your device’s specifications as well.

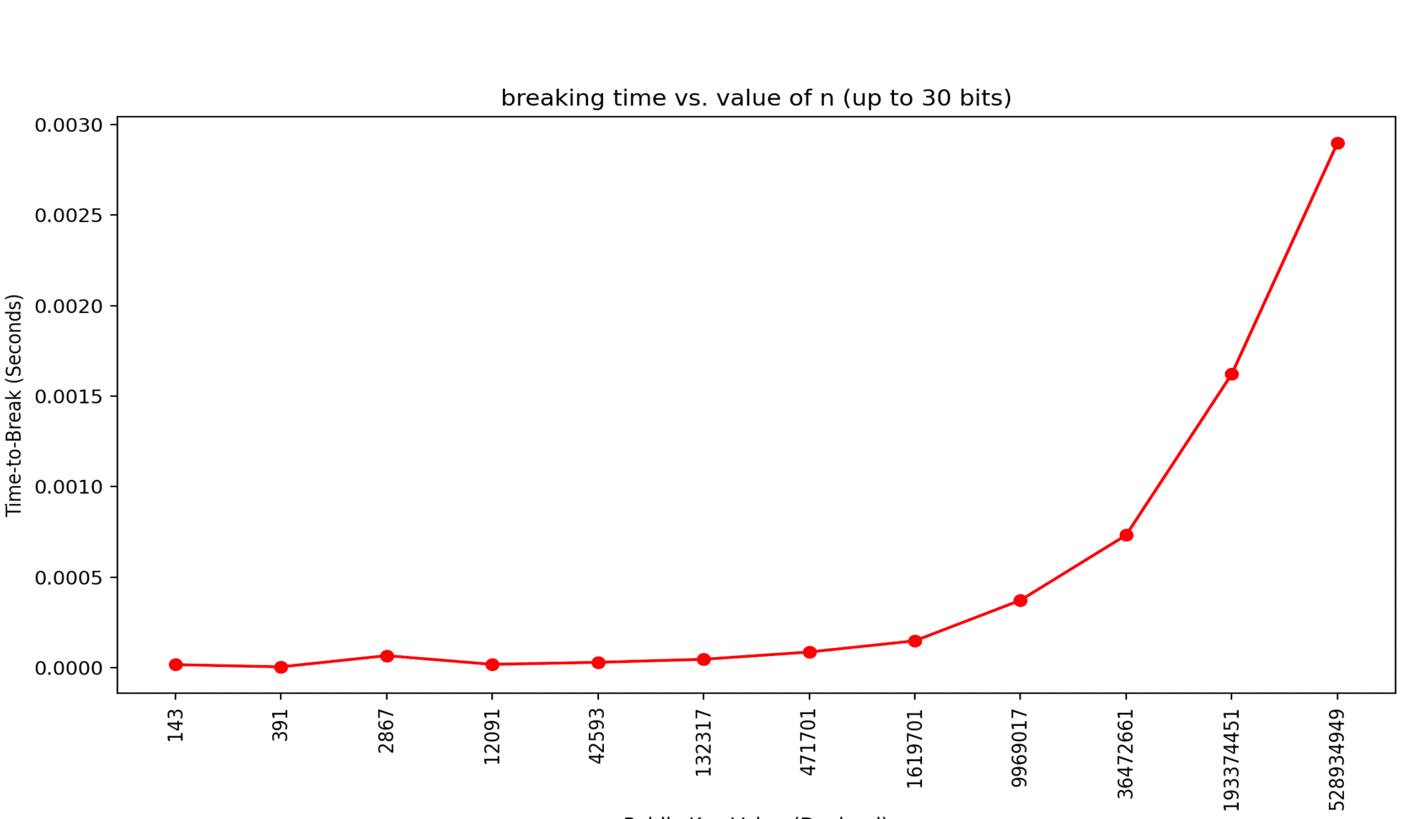
### RSA Mathematical Brute-force Attack Analysis



In the mathematical brute-force attack (explained earlier.) We started by setting up an array of public keys of length 8, 12, …, 1024 we then ran the factoring algorithm on the whole array and reported the time results in a text file. We kept trying to break the keys for more than 450 minutes (7.5 hours) in this period we were able to break keys up to 74 bits (and it took as much as 3.33 hours to break the 74-bit key).

Notice that although it seems that the time for breaking smaller is the same (the flat region on the left.), it’s not actually flat but it’s just that the scale on y is large due to the time taken to break the very large keys. In particular, this is what we get if stop when the key-length hits 46 bits.



And this is what we get

If we stop when the key length hits 30 bits. The trend is overall clearly exponential which is indeed the known time complexity of prime factorization. Notice that we were easily able to break RSA for 74 bits which means that unlike symmetric encryption we can’t use such small key-lengths which justifies why we resorted to using 256-bit RSA in our algorithm’s implementation (which as far as we believe has not been broken by a normal computer so far.)

The computer used for this test was the Macbook M1 Pro which has specifications

|  |  |
| --- | --- |
| Processor & GPU | Apple M1 Chip (2.1 – 3.2 GHz) |
| Processor Cores | 8 Cores (4 performance cores and 4 efficiency cores) |
| Memory | LPDDR4X 8 GB RAM |

## Further Notes

## 