Report Project 2 - William Lewin & Elias Chahine wlewin@kth.se, echahine@kth.se

Summary

Task

Professor Alice is sending a problem to the student Bob according to the procedure in section 1.1.1. You are supposed to solve Bob's problem. However, you need to start by cracking the cipher sent to Bob. When translating to ASCII, you can assume the base 256.

The numbers is the list seems to be of the same size. Why?
Motivate your selected mathematical model!

Task derived from previous task:

Congratulations! You have now managed to crack the RSA cipher. Your task is as follows: write a method R
SAcrack[cipher, n, e] that w "ill crack a standard RSA cipher and delivers clear text from the string cipher
. When you are finished with your method, you should " investigate how long it will take to crack the ciph
er of the Swedish text DISKRET MATTE, DE E FETT NAIS! for different sizes on y
our public key n (100–200 bits). Visualize your results in a proper graph. It is very important that you
study the section 2.3 in the instructions. Your graph should lead you to a model where you can predict
how long it would take to crack a cipher if n is 1024, 2048 bits or 4096 bits with your computer.

1.1.1 Using RSA for Authentication

In RSA it's not just Alice that can send a message to Bob. Anyone that access Bob's public keys can sen an encrypted message. So how can Bob know that the message is from Alice?

A rather straight forward way of doing this is that Alice also encrypt the message with her secret key d_{Alice}. Bob will later decrypt, using Alice's public key.

Let's say Alice wants to send a message to Bob.

- $m_{\text{Alice}} < \min(n_{\text{Alice}}, n_{\text{Bob}})$
- start with the key that belongs to $\min(n_{\text{Alice}}, n_{\text{Bob}})$
  - $n_{\text{Alice}} < n_{\text{Bob}} \Rightarrow c_0 \equiv_{n_{\text{Alice}}} m_{\text{Alice}}^{d_{\text{Alice}}},\ c_{\text{Alice}} \equiv_{n_{\text{Bob}}} c_0^{e_{\text{Bob}}}$
  - $n_{\text{Bob}} < n_{\text{Alice}} \Rightarrow c_0 \equiv_{n_{\text{Bob}}} m_{\text{Alice}}^{e_{\text{Bob}}},\ c_{\text{Alice}} \equiv_{n_{\text{Alice}}} c_0^{d_{\text{Alice}}}$

Bob decrypts the cipher by

- start with the key that belongs to $\max(n_{\text{Alice}}, n_{\text{Bob}})$
  - $n_{\text{Bob}} > n_{\text{Alice}} \Rightarrow c_1 \equiv_{n_{\text{Bob}}} c_{\text{Alice}}^{d_{\text{Bob}}},\ m_{\text{Alice}} \equiv_{n_{\text{Alice}}} c_1^{e_{\text{Alice}}}$
  - $n_{\text{Alice}} > n_{\text{Bob}} \Rightarrow c_1 \equiv_{n_{\text{Alice}}} c_{\text{Alice}}^{e_{\text{Alice}}},\ m_{\text{Alice}} \equiv_{n_{\text{Bob}}} c_1^{d_{\text{Bob}}}$

Usually the authentication is not done on the full message, but rather a message digest or a cryptographic checksum, e.g. secure hash algorithm (SHA).

Result

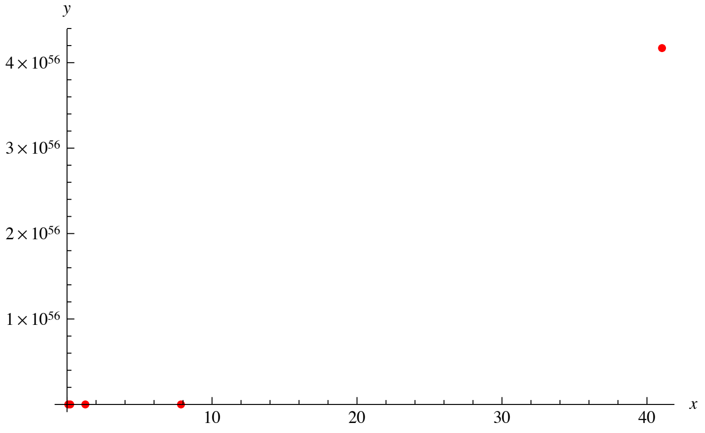
The numbers in the cipher are roughly of the same size because the message needs to be broken down in to smaller pieces (smaller than n) in order for the cracking method to return a unambiguous result.

After cracking the initial RSA puzzle, we were introduced to a new task. This task involved writing a method for decrypting a cipher and calculating the time required to crack the cipher depending on the size of the size of the public key (N).
The time required to crack the cipher will strongly depend on the size of N, seeing as the main problem of cracking an RSA cipher is the prime factoring required to reverse the encryption process.

Approx N.	Processing time
$2^{100-110}$	0.087013
$2^{120-130}$	0.218892
$2^{140-150}$	1.26341
$2^{160-170}$	7.85949
$2^{180-190}$	41.0367

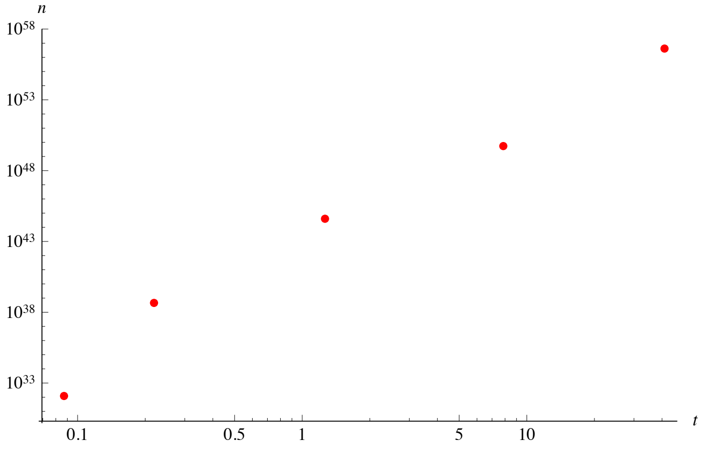
Our mathematical model of choosing was a power function. As the graph below shows, when plotted as a standard graph, the values show an exponential curve upwards.

Standard plotted graph

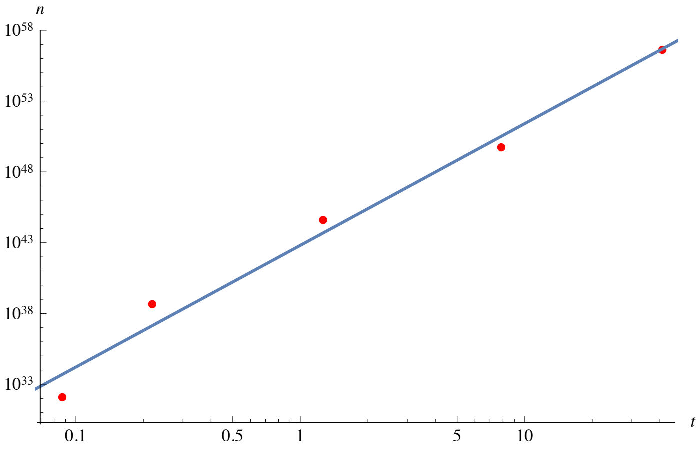


When plotted as a log-log graph, the values are displayed as a straight line. We chose this model based on “If data fits a straight line in a log(y)-log(x) plot, then the model is a power function.”

Log-log graph



Log-log and function graph



Based on this model and the data we have gathered, a prediction of the running time of larger N was created.

N	Estimated processing time
2^{1024}	4.94737×10^{68}
2^{2048}	1.91796×10^{71}
2^{4096}	7.43538×10^{73}

Code