

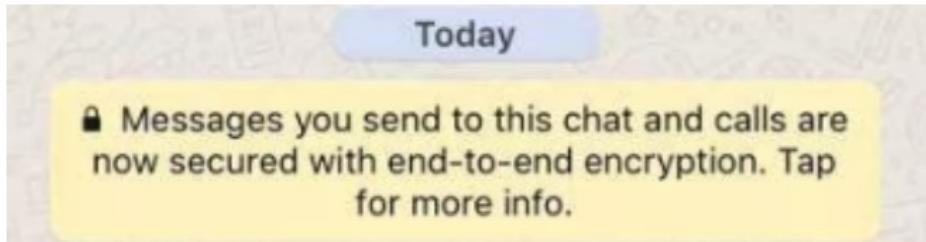
# How to Win a 1,000,000\$ (or at Least a Cookie) through Cryptography: Computational Analysis of the Security of the RSA Encryption Algorithm

Andrey Ambartsumov

Supervised by Professor Takei

May 8th, 2024

# Why Cryptography



Log In

Email Address

Password

Remember me for 30 days

**Log In**

or

 Sign in with Google

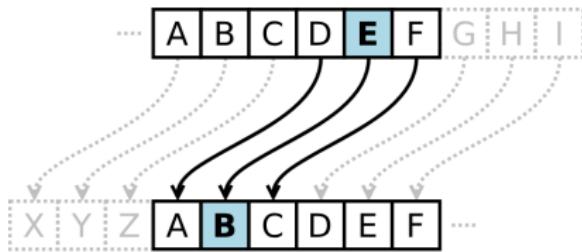
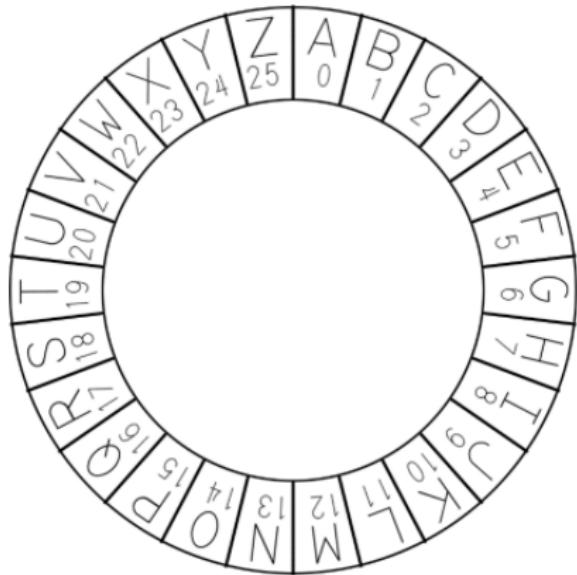
Forgot your password?

# Caesar Cipher - Julius Caesar, the first Cryptographer

Julius Caesar invented the Caesar Cipher in 100BC.



# Caesar Cipher - Example



<https://ceasarcipher.onrender.com/>

# RSA - Analogy



# RSA - Analogy



# RSA - Analogy



# RSA - Analogy



# RSA - Explanation



Public Key Pair



Private Key

## RSA - Send a Secret

Bob's Public Keys: (33, 7)

Alice:  $G \rightarrow 6$

## RSA - Send a Secret

Bob's Public Keys:  $(33, 7)$

Alice:  $G \rightarrow 6$

$$\begin{aligned} 6^7 &= 279936 \\ &= 33 \cdot 8482 + 30 \\ &\equiv 30 \pmod{33} \end{aligned}$$

Alice sends 30 to Bob through a public channel

## RSA - Send a Secret

Bob's Public Keys: (33, 7)

Alice:  $G \rightarrow 6$

$$6^7 = 279936$$

$$= 33 \cdot 8482 + 30$$

$$\equiv 30 \pmod{33}$$

On Bob's side, he has the secret key 3:

$$30^3 = 27000$$

$$\equiv 6 \pmod{33}$$

Alice sends 30 to Bob through a public channel

## RSA - Choosing the Keys

- ▶ Encryption modulus:  $33 = 3 \times 11$
- ▶ Encryption and Decryption Exponents:

$$\textcolor{red}{7} \cdot \textcolor{green}{3} = (3 - 1)(11 - 1)n + 1$$

$$21 = 20n + 1$$

$$21 \equiv 1 \pmod{20}$$

# RSA - Security

Bob's public keys:  $(33, 7)$

Alice wants to send 6

she computes  $6^7 \equiv 30 \pmod{33}$

she sends 30 to Bob

Bob has the secret key 3 and computes

$30^3 \equiv 6 \pmod{33}$

## 1. $n^{th}$ roots in modular

$$m^7 = 33n + 30$$

$$m = \sqrt[7]{33n + 30}$$

$$6 = \sqrt[7]{33 \cdot 8482 + 30}$$

# RSA - Security

Bob's public keys:  $(33, 7)$

Alice wants to send 6

she computes  $6^7 \equiv 30 \pmod{33}$

she sends 30 to Bob

Bob has the secret key 3 and computes

$30^3 \equiv 6 \pmod{33}$

## 1. $n^{th}$ roots in modular

$$m^7 = 33n + 30$$

$$m = \sqrt[7]{33n + 30}$$

$$6 = \sqrt[7]{33 \cdot 8482 + 30}$$

## 2. Factorize the encryption modulus into p and q

$$33 = 3 \times 11$$

# RSA - Security

Bob's public keys:  $(33, 7)$

Alice wants to send 6

she computes  $6^7 \equiv 30 \pmod{33}$

she sends 30 to Bob

Bob has the secret key 3 and computes

$30^3 \equiv 6 \pmod{33}$

## 1. $n^{th}$ roots in modular

$$m^7 = 33n + 30$$

$$m = \sqrt[7]{33n + 30}$$

$$6 = \sqrt[7]{33 \cdot 8482 + 30}$$

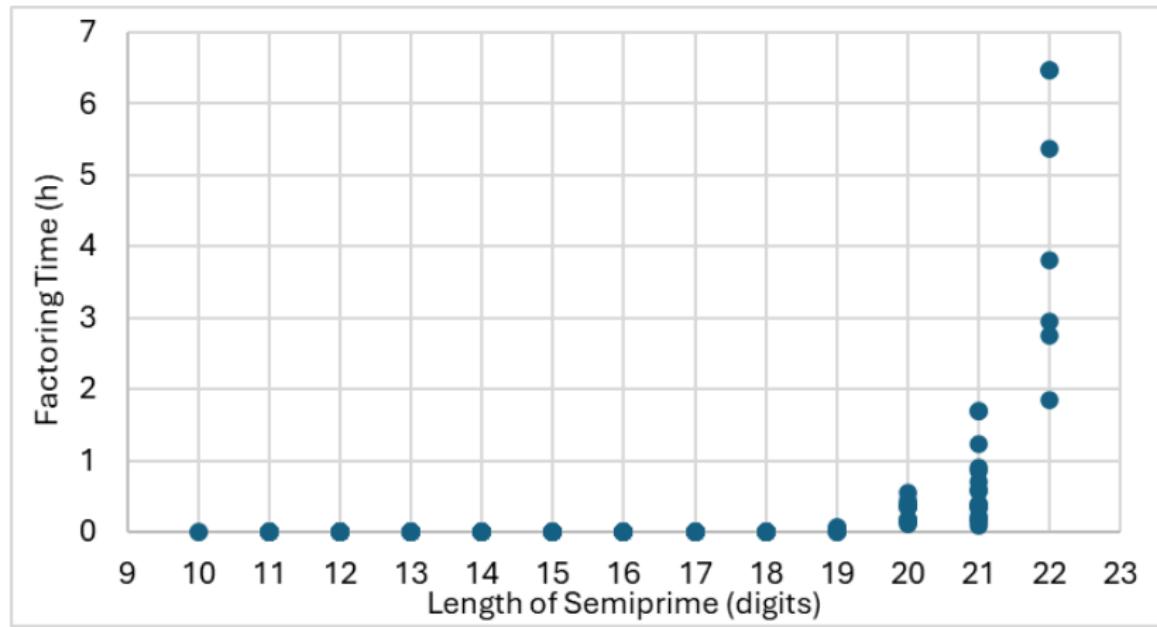
## 2. Factorize the encryption modulus into p and q

$$33 = 3 \times 11$$

$$7 \cdot \text{key} = (3 - 1)(11 - 1)n + 1$$

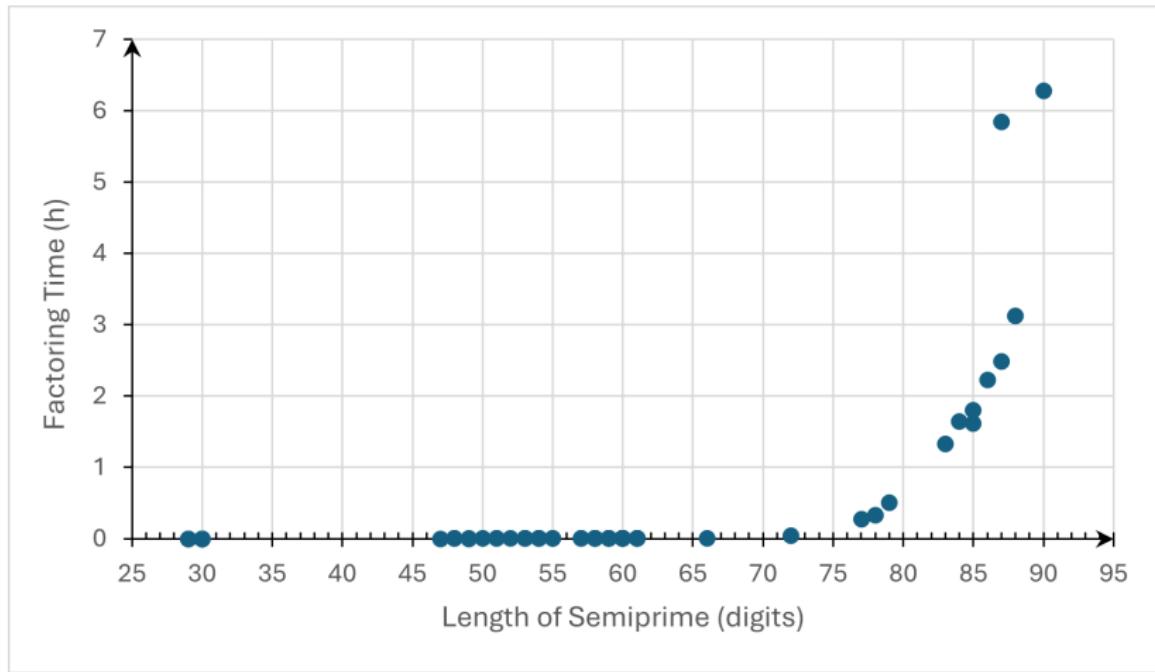
$$\text{key} = 3$$

# RSA - Trial and Error Factorization using Python



Factorization time of semiprimes using trial and error

# RSA - Quadratic Sieve using C++



Factorization time of semiprimes using the Quadratic Sieve

## RSA - 90 digits semiprime

Encryption takes:

0.0009973 seconds

Decryption takes:

0.0008678 seconds

This semi-prime took 7 hours to factorize:

601348911492967474716626562591162015444606322948636213  
084003067539621391421673708075577  
= 88074813197177059161356775912755702665358209  
x  
6827705784021369734890122252355572751354553

## RSA - 309 digits Encryption Modulus

An industry standard would be:

14378324890482304582689541244275156569918126704352715981  
07249824368398178285945362131773362655027756794178034116  
11160543281251113007493405658260634371576346949950420305  
13653485026571402371334634743436045171775186957620382841  
73906148107290849160323765547206418773039754189427597424  
67109810412421095487606337209

# Decrypting Challenges!

Head onto:

[www.cookiechallenge.live](http://www.cookiechallenge.live)

To have a chance to win cookies!

Good luck!