AUGUST 2025. BJÖRN HALLSTRÖM AND JOHN PROSSER

Encryption Tool Project

NOD CODING BOOTCAMP PROJECT 1

Caesar! We have problem!

Those pesky Greeks are intercepting your messages to the generals!

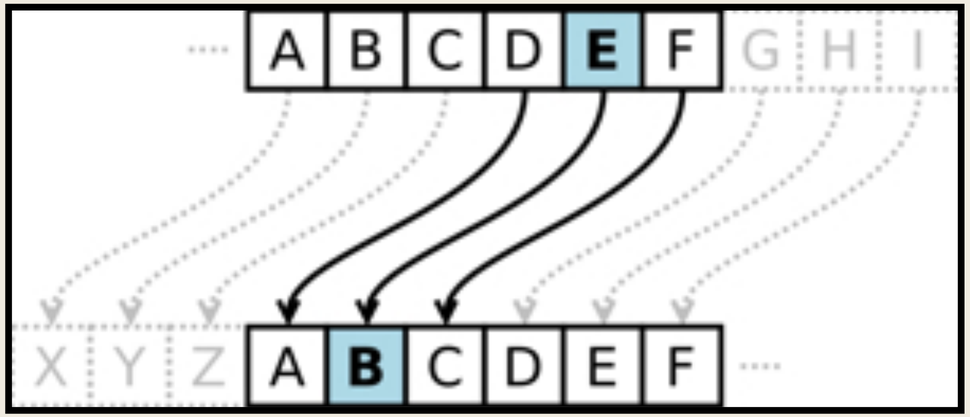
Solution: The Caesar Cipher!

Let's shift all letters in the alphabet to a different letter using a key, so the message is unreadable!

The generals in the field can recover the message by using the same key.

Example: Key = -3

Shift all letter's down by 3.



"hello world" becomes "ebiil tloia"

Caesar! We have another problem!

Computers have rendered your cipher completely useless!

1. A modern computer could easily discover the key by quickly testing all possible options

2. Even if that wasn't the case, how can we exchange a key over the internet in the first place?

Solution: RSA Encryption!

RSA encryption uses an integer factorisation problem that digital computers find very difficult to solve.

Factoring numbers is hard!

What are the prime factors of

n = 7470451395944986
2836995744930144829 2019?

Solution: RSA Encryption!

RSA encryption uses an integer factorisation problem that digital computers find very difficult to solve.

Factoring numbers is hard!

What are the prime factors of

n = 7470451395944986
2836995744930144829201 9?

Answer:

p = 2305843009213693951 1
q = 3241619000711725562 9

Solution: RSA Encryption!

RSA encryption uses an integer factorisation problem that digital computers find very difficult to solve.

Moreover, the encryption is asymmetric: different keys are used to encrypt and decrypt.

Factoring numbers is hard!

What are the prime factors of

n = 7470451395944986 2836995744930144829201 9?

Answer:

p = 2305843009213693951 1
q = 3241619000711725562 9

Solution: RSA Encryption!

RSA encryption uses an integer factorisation problem that digital computers find very difficult to solve.

Moreover, the encryption is asymmetric: different keys are used to encrypt and decrypt.

I can share the 'public key' with everyone to use for encryption.

I keep my 'private key' to use for decryption.

Factoring numbers is hard!

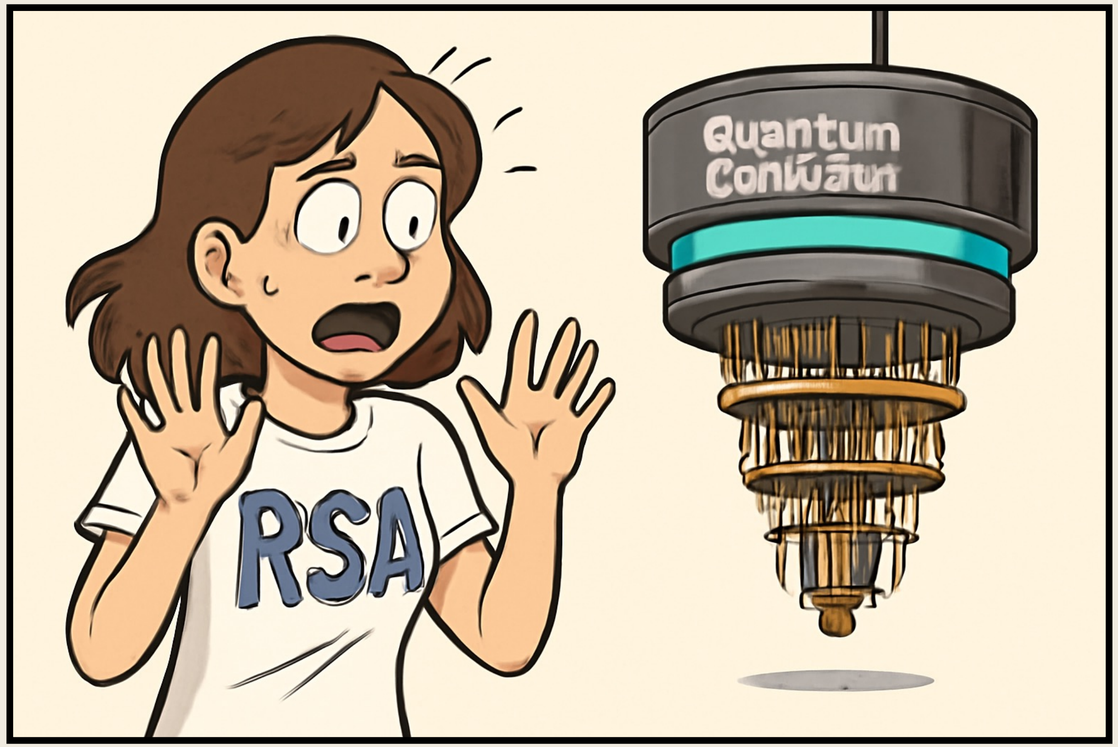
What are the prime factors of

n = 7470451395944986
2836995744930144829 2019?

Answer:

p = 2305843009213693951 1
q = 3241619000711725562 9

Caesar! We have a new problem!



Factoring of integers is easy if you have a quantum computer. This would make RSA encryption easy to break.

Development of quantum secure encryption algorithms is an important feature we need to add in the future!