HW4 Bignum

Assignment explanation and optimization ideas

Bignum class

HW4 Part1

- Vector with base 10 representation
- Operations:
  - +
  - -
  - *
  - /
  - %
  - expmod

Encryption & decryption

HW4 Part2

expmod

Encryption: $m^{(rsa_e)} \% (rsa_n)$

Decryption: $m^{(rsa_d)} \% (rsa_n)$

Text file Read

HW4 Part2

The cake is a lie!

The cake is a lie!

The cake is a lie! The cake is a lie!

std::cin

Line-by-line

The cake is a lie!

The cake is a lie!

The cake is a lie! The cake is a lie!

Process line

Text file Preprocess

HW4 Part2

Process line

1The cake is a lie!	1
2The cake is a lie!	2
3The cake is a lie! The cake is a lie!	3

Padding to 96 chars

Total char 96+6=102
(line number on both sides takes 3 digits each)

Form Bignums

Text file Encryption

Truncate each line to two 51 chars arrs

1The cake is a lie!	1
2The cake is a lie!	2
3The cake is a lie! The cake is a lie!	3

Process line

1.....	1
2.....	2
3.....	3

Transfer each char to 3-digit ASCII decimal code

Run Bignum Encryption

1.....	1
2.....	2
3.....	3

Run Bignum expmod

Bignum(1.....) . expmod(rsa_e, rsa_n)

Bignum(.....1) . expmod(rsa_e, rsa_n)

Bignum(2.....) . expmod(rsa_e, rsa_n)

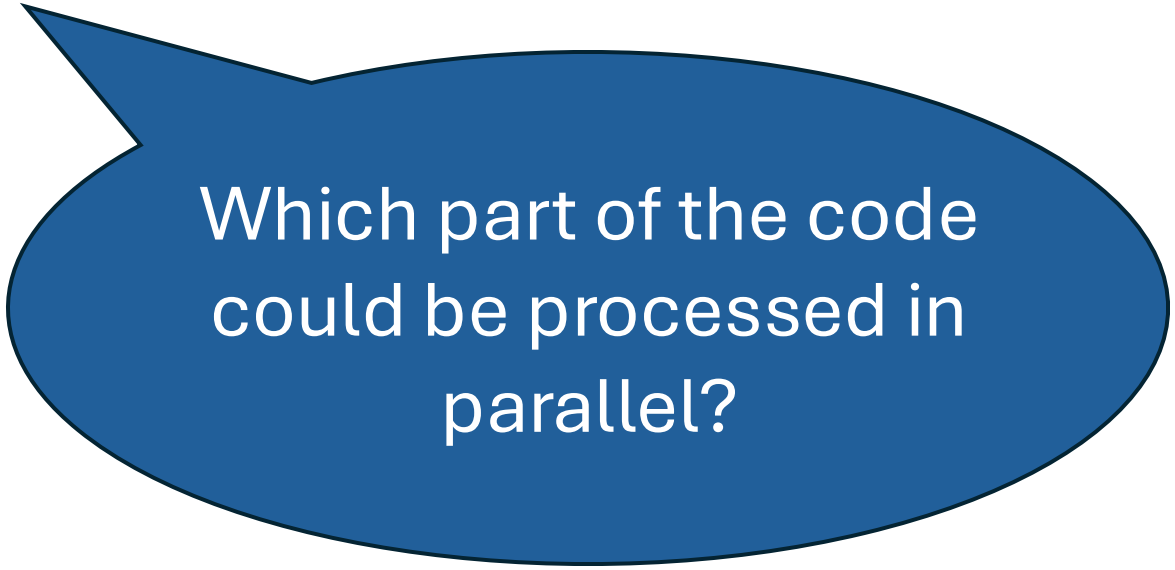
Bignum(.....2) . expmod(rsa_e, rsa_n)

Bignum(3.....) . expmod(rsa_e, rsa_n)

Bignum(.....3) . expmod(rsa_e, rsa_n)

Optimizations

- Multi-threading



More ideas: https://docs.google.com/spreadsheets/d/1eXCRs8yoYUj5jrFATFsYL0elqgL5QaTlSrly-_QkAzQ/edit?gid=0#gid=0