University of New Haven

TAGLIATELA
COLLEGE OF ENGINEERING

Encryption Algorithm Comparison

CSCI-2246-01 Introduction to Computer Security
Spring 2021

Justin Hollman, Orion Duffy, Ahmed Muntasir Hossain

Introduction

- Encryption Algorithms are used to change data in a predictable way using a key so that it cannot be read without decrypting it with the correct key
  - Symmetric Key Encryption: same key is used for encryption and decryption
  - Asymmetric Key Encryption: different keys are used for encryption and decryption

- Developed an application in C++ to test the speed of
  - Symmetric key encryption algorithms: AES and 3DES
  - Asymmetric key encryption algorithm: RSA

- Compared the costs and benefits of each type of encryption algorithms

Analysis - Algorithm

- Imported an open-source library used by professional developers called Crypto++
- Compiled the cryptopp.lib file to include the headers for AES, 3DES, and RSA encryption algorithms
- Developed the code in C++ which included:
  - Plaintext
  - Encryptor
  - Print ciphertext
  - Decryptor
  - Print decryptedtext

Analysis - Time

- Used chrono library to measure the time for encryption and decryption
  - Ran several encryption and decryption processes for each algorithm
  - Printed the time taken for encryption and decryption on each run
  - Computed the total time and calculated the average of all the runs for each algorithm

- Expected RSA to take a significantly longer time to run than AES and 3DES
  - Results support our hypothesis

Symmetric Key - Duration

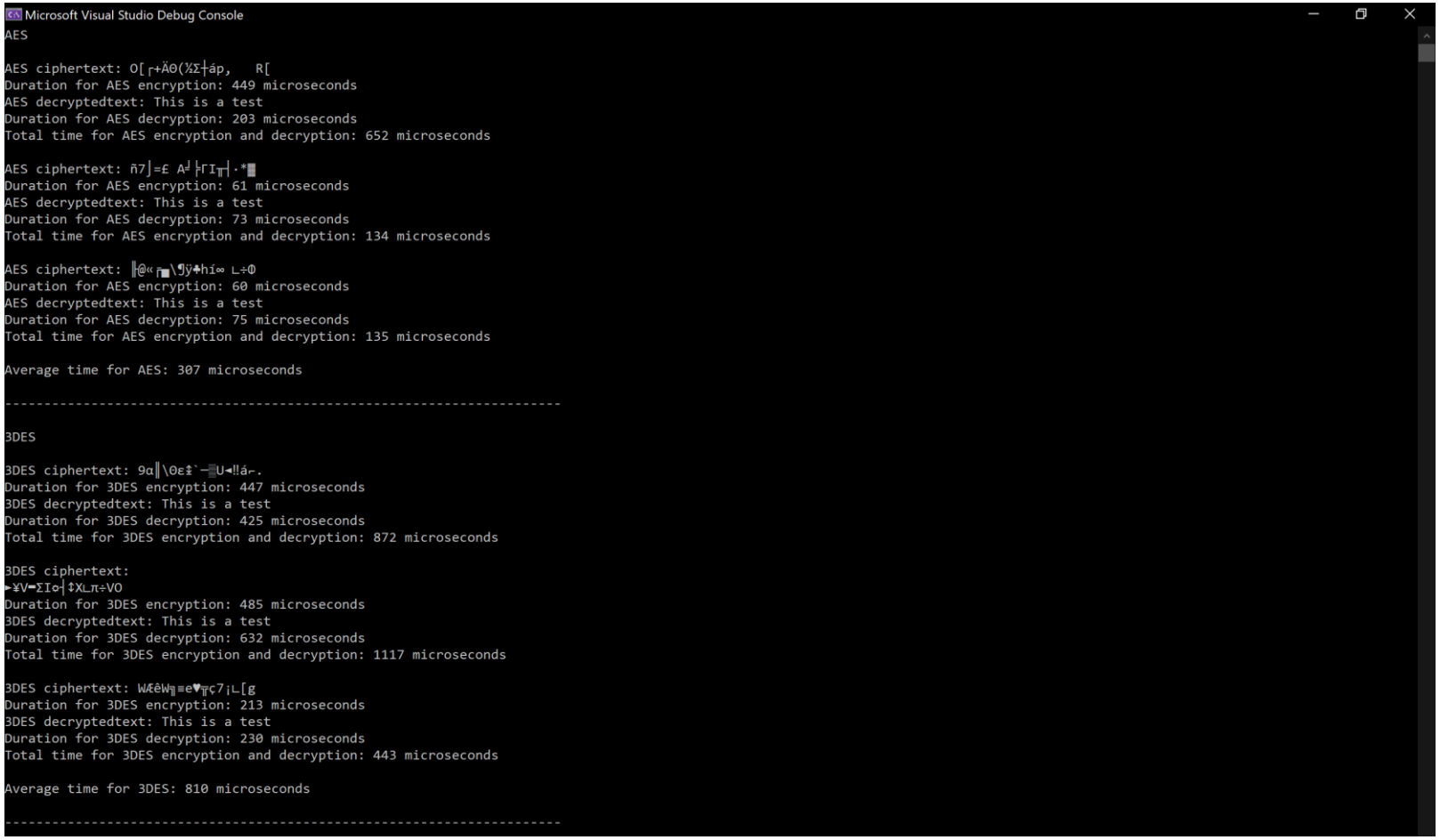
AES	Encryption Time (µs)	Decryption Time (µs)	Total Time (µs)
Run 1	449	203	652
Run 2	61	73	134
Run 3	68	75	135
Average Time	193	117	307

3DES	Encryption Time (µs)	Decryption Time (µs)	Total Time (µs)
Run 1	447	425	872
Run 2	485	652	1117
Run 3	213	230	443
Average Time	382	436	810

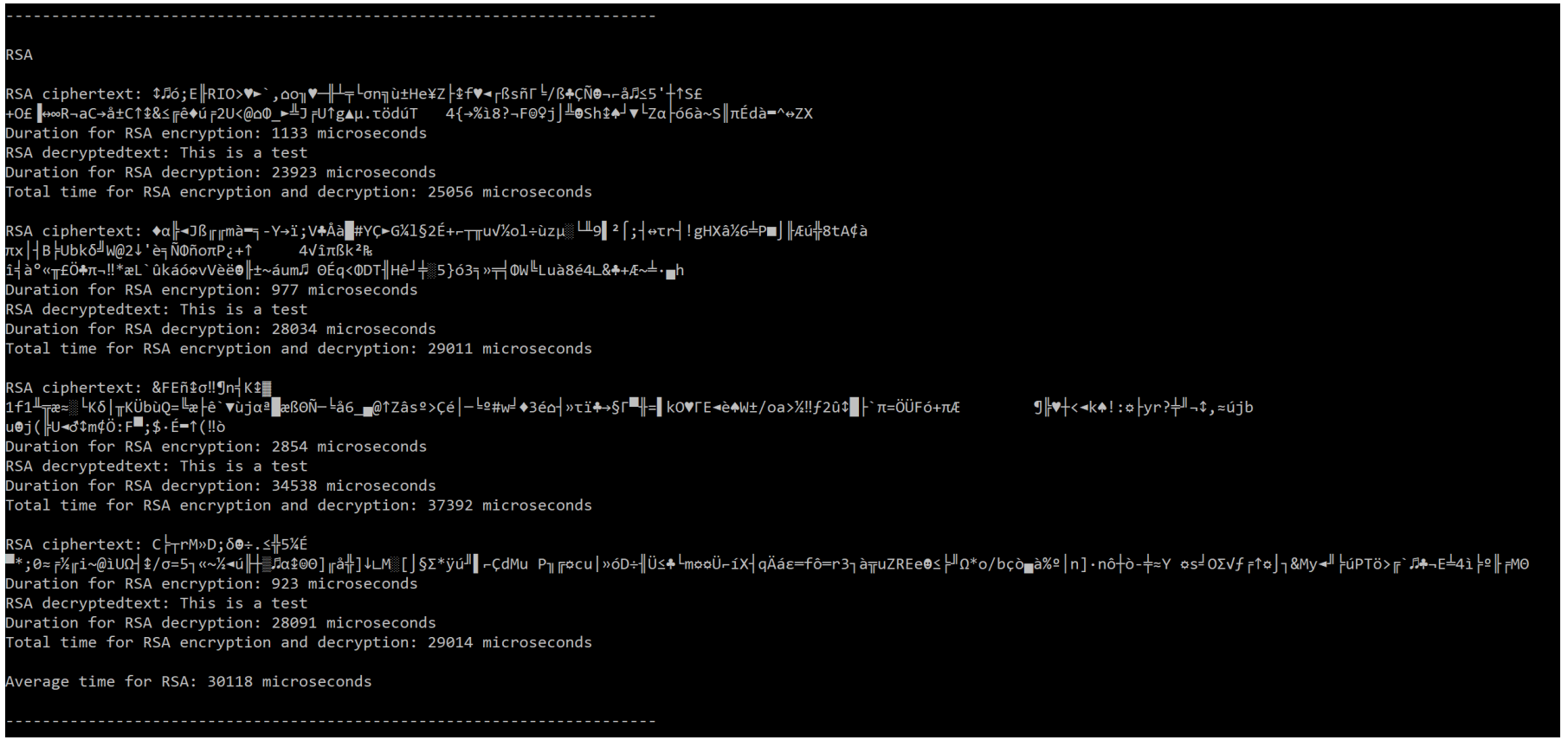
Asymmetric Key - Duration

RSA	Encryption Time (µs)	Decryption Time (µs)	Total Time (µs)
Run 1	1133	23923	25056
Run 2	977	28034	29011
Run 3	2854	34538	37392
Run 4	923	28091	29014
Average Time	1472	21624	30118

Symmetric Key Results C++



Asymmetric Key Results C++



Impact on Computer Security

- Symmetric key encryption is faster
  - The key must be transferred to the other party

- Asymmetric key encryption is far, far, slower
  - Sharing the key that allows decryption is not necessary

- Symmetric key encryption is used for large quantities of data
- Asymmetric key is more reasonable for small quantities
  - Asymmetric key encryption is often used to transfer the key for symmetric key encryption

Conclusions

- Encryption and decryption done using Crypto++ library
- Tested AES, 3DES and RSA algorithms
- Compared their performance and times
- Symmetric key algorithm is faster
- Asymmetric key algorithm is slower but does not require the user to share the key

GitHub

- https://github.com/muntasir-hossain314159/Encryption-Algorithm-Comparison

Thank You