



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++

```
Microsoft Visual Studio Debug Console
AES
AES ciphertext: 0[r+Ä0(½Σ+áp, R[
Duration for AES encryption: 449 microseconds
AES decryptedtext: This is a test
Duration for AES decryption: 203 microseconds
Total time for AES encryption and decryption: 652 microseconds

AES ciphertext: ñ7]=É A^ |rI|.*
Duration for AES encryption: 61 microseconds
AES decryptedtext: This is a test
Duration for AES decryption: 73 microseconds
Total time for AES encryption and decryption: 134 microseconds

AES ciphertext: ||@«\jy+hi» L+0
Duration for AES encryption: 60 microseconds
AES decryptedtext: This is a test
Duration for AES decryption: 75 microseconds
Total time for AES encryption and decryption: 135 microseconds

Average time for AES: 307 microseconds
-----

3DES
3DES ciphertext: 9a||\0e±`-U!lá-.
Duration for 3DES encryption: 447 microseconds
3DES decryptedtext: This is a test
Duration for 3DES decryption: 425 microseconds
Total time for 3DES encryption and decryption: 872 microseconds

3DES ciphertext:
~YV~XI0~}XLπ+V0
Duration for 3DES encryption: 485 microseconds
3DES decryptedtext: This is a test
Duration for 3DES decryption: 632 microseconds
Total time for 3DES encryption and decryption: 1117 microseconds

3DES ciphertext: WÆêWjme♥qç7jL[g
Duration for 3DES encryption: 213 microseconds
3DES decryptedtext: This is a test
Duration for 3DES decryption: 230 microseconds
Total time for 3DES encryption and decryption: 443 microseconds

Average time for 3DES: 810 microseconds
-----
```

# Asymmetric Key Results C++

```
-----
RSA
RSA ciphertext: 3B6;E[RIO>v` ,a0q1v-||T-LonqÛ±He¥Z|±f▼◀rBsñΓL/B♣ÇÑ0~râB≤5'†↑SE
+0E [∞∞R~aC→â±C†±&≤fê♦úf2U<@o0_>♯J fU†g▲μ.tôdúT 4{→%i8?-F09j]±0Sh±♣J▼LZα|ó6â~S||πÉdà~^↔ZX
Duration for RSA encryption: 1133 microseconds
RSA decryptedtext: This is a test
Duration for RSA decryption: 23923 microseconds
Total time for RSA encryption and decryption: 25056 microseconds

RSA ciphertext: ♦α||-∅B||rma-γ-Y→i;V+Ââ||#YÇ◀G%l$2É+~T||uv%ol÷üzμ||L9||²[;|↔tr|!gHXâ%6±P||||Æú||8tA$à
πx|↓B|Ubkδ||W@2↓'èqN0ñonP;+↑ 4v1πBk²R
i↓à°«Tf0+π-!!*æL`ùkáóovVèè0||±~áumJ 0Éq<0DT||Hê↓±||5}ó3γ»||0W||Luà8é4L&+±Æ~±.h
Duration for RSA encryption: 977 microseconds
RSA decryptedtext: This is a test
Duration for RSA decryption: 28034 microseconds
Total time for RSA encryption and decryption: 29011 microseconds

RSA ciphertext: &FEñ$σ!!9n|K$
1f1||æ=||Kδ|TtKÛbûQ=||æ|è`▼úja||æB0Ñ~Lâ6_||@↑Zâse>Çé|~Læ#w||♦3éα|»ti+→$Γ||=||k0vΓE~è♣W±/oa>%!!f2û$|||π=ÖÜFó+πÆ 9||♥|<◀k♠! :ø|yr?±||~$,=újb
u0j<||U~ø$m$0:F||;$·É=↑(!!ò
Duration for RSA encryption: 2854 microseconds
RSA decryptedtext: This is a test
Duration for RSA decryption: 34538 microseconds
Total time for RSA encryption and decryption: 37392 microseconds

RSA ciphertext: C|TrM»D;δ0+~.≤||5%É
||*;0= f%|ri~@iUΩ|±/σ=5γ«~%ú|||±||Bα±00]||râ||]↓LM||[|]S$*ÿú|||~ÇdMu P||fæcu|»óD÷|Ü≤♣LmoeÜ~iX|qÃâε=fô=r3γàTtuZREe0≤||Ω*o/bçð||à%²|n]·nô|ò-†=Y 0sJ0Sv f f†ø]γ&My◀|||↑üPTö>||r`B♣~E±4i|f²||fMO
Duration for RSA encryption: 923 microseconds
RSA decryptedtext: This is a test
Duration for RSA decryption: 28091 microseconds
Total time for RSA encryption and decryption: 29014 microseconds

Average time for RSA: 30118 microseconds
-----
```



# 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**