Emin Musayev

Robert Cacho Ruiz

Jingyi Wang

April 20, 2021

Project Report (AES, DES, 3DES)

Code: **https://github.com/freshskates/Encryption-Testing-Zone**

Prompt:

- Measure and compare the time taken for encryption and decryption using DES, 3DES and AES, with different input sizes. Analyze the three algorithms and identify which component(s) made an algorithm particularly fast/slow, weak/strong. You can implement your own algorithms or use others' implementation. (You can use external library).

Understanding the Concept: What is Encryption?

Symmetric-Key Encryption Explanation

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. The keys may be identical, or there may be a simple transformation to go between the two keys.

Public-Key Encryption Explanation

Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key.

Overview

To analyze our AES and DES we used python, along with the pyaes and des library that we imported. We timed both the encryption and decryption individually using wrappers in python. We dumped the data into a file which contains the same keys being encrypted and decrypted with the different algorithms which are AES, DES and 3DES.

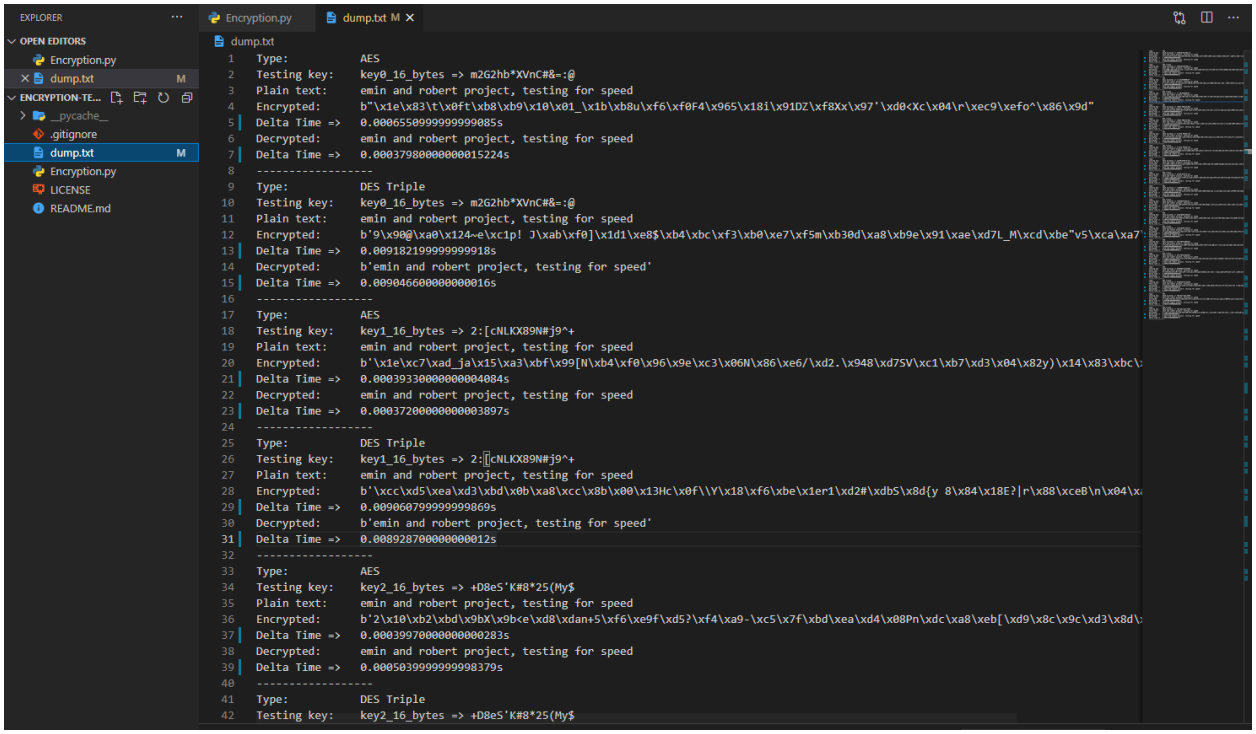
Analysis

DES, 3DES and AES were tested and analyzed for this project. We coded the testing zone in python. DES is short for Data Encryption Standard, and it is a symmetric key algorithm for the encryption of digital data.

Overall AES is faster and better than DES and 3DES. It can encrypt faster along with having better security.

```
Testing key:    key0_16_bytes: m2G2hb*XVnC#&=:@
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.000798 seconds
Encrypted:      (b"\x1e\x83\t\x0ft\xb8\xb9\x10\x01_\x1b\xb8u\xf6\xf0F4\x965\x18i\x91DZ\xf8Xx\x97'\xd0<Xc\x04\r\xec9\xefo^\x86\x9d", 0.0007978000000001817)

T decrypt =>    Elapsed: 0.000408 seconds
Decrypted:      ('emin and robert project, testing for speed', 0.00040839999999997545)
------------------
Testing key:    key1_16_bytes: 2:[cNLKX89N#j9^+
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.000404 seconds
Encrypted:      (b'\x1e\xc7\xad_ja\x15\xa3\xbf\x99[N\xb4\xf0\x96\x9e\xc3\x06N\x86\xe6/\xd2.\x948\xd7SV\xc1\xb7\xd3\x04\x82y)\x14\x83\xbc\xfc\xec\xa4', 0.0004037999999999542)

T decrypt =>    Elapsed: 0.000375 seconds
Decrypted:      ('emin and robert project, testing for speed', 0.00037509999999985055)
------------------
Testing key:    key2_16_bytes: +D8eS'K#8*25(My$
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.000397 seconds
Encrypted:      (b'2\x10\xb2\xbd\x9bX\x9b<e\xd8\xdan+5\xf6\xe9f\xd5?\xf4\xa9-\xc5\x7f\xbd\xea\xd4\x08Pn\xdc\xa8\xeb[\xd9\x8c\x9c\xd3\x8d\x90\xccF', 0.0003972000000000975)

T decrypt =>    Elapsed: 0.000369 seconds
Decrypted:      ('emin and robert project, testing for speed', 0.00036869999999988856)
------------------
Testing key:    key3_16_bytes: Z;Y2Fe.PNx8h~]eV
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.000381 seconds
Encrypted:      (b'\x12\x85\xad\xaa\x88:\xae\xf6\xec\xe4\x98X\xd8\xcd4\\ym\x1c1)\xb0\x18|\x7f]\xda\xfcr\xacGiXJ\xae\xd2T\x9d\x07\x02\x07\x8e', 0.0003805000000011686)

T decrypt =>    Elapsed: 0.000367 seconds
Decrypted:      ('emin and robert project, testing for speed', 0.0003672999999999593)
------------------
Testing key:    key4_16_bytes: pt4YNLb9+M^m^w**
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.000451 seconds
Encrypted:      (b'2\x015/\x99\xcf\xf3[\xdb\xe2DQs\x0c\xf3\xc0jL\x993\xb8\xf8\xbdkM\xa1gyX\xb2\xb1\xab\x81=\xe6\xca\xf2\xfc\x9c[L\xdc', 0.0004511000000000376)

T decrypt =>    Elapsed: 0.000420 seconds
Decrypted:      ('emin and robert project, testing for speed', 0.0004200999999999233)
------------------
Testing key:    key5_16_bytes: x4eRGWXFv56m=E-x
Plain text:     emin and robert project, testing for speed
```

```
------------------
Testing key:    key9_16_bytes: YQ3!@2vr6y2!4dV9
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.009128 seconds
Encrypted:      (b'\xd2\x15\xeb\xb2\xeb\xd0\x00\xdf\x07EW\xfc\xd7QN\x7f_\xc6\x98\r\xb6\xdf\xe2z,|\xeb!\xe0\xe0\xaa\xb1{\x14U\x08\xf0k\xfe\x9b\x7f\xdc\xfd\xef\x9d\x14\x83\xcb
', 0.009127600000000013)

T decrypt =>    Elapsed: 0.008919 seconds
Decrypted:      (b'emin and robert project, testing for speed', 0.008918600000000011)
------------------
Testing key:    single: some key
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.003093 seconds
Encrypted:      (b'\x15N(\xc8\r\xc0X\xff&-m\x8e\x16\x16\xb9Z\xc0wY\xa9I\x8cgLV~TU\x8f\x11{\xd6$7L\xa1\x92E3u3_\x02\xfe\x84\xd8\xb9\xbc', 0.003092600000000001)

T decrypt =>    Elapsed: 0.003475 seconds
Decrypted:      (b'emin and robert project, testing for speed', 0.0034750999999999532)
------------------
Testing key:    triple: a key for TRIPLE
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.008959 seconds
Encrypted:      (b'1\xbd\x92\x1aqt\xe6\xb1\x05,\x9b\\,\xeb\x88\x86\xc8\xe56\x11\xd8\x19\xa0\x9c\x8b\xc7\x00\xcbE\xccT\x90\xf0v\x03c8\x0b\xb5y!\xf8\xa1,\xc1\xd8\x05%', 0.0089
58800000000045)

T decrypt =>    Elapsed: 0.008960 seconds
Decrypted:      (b'emin and robert project, testing for speed', 0.008959900000000002)
------------------
Testing key:    bytes_24: a 24-byte key for TRIPLE
Plain text:     emin and robert project, testing for speed

T encrypt =>    Elapsed: 0.009244 seconds
Encrypted:      (b"\xa4T\x7f\xd3p8\x8c\xcbh\xf4 \x9d\x94\xaefV\xec\xdd\x98\x1b.)oq]\xc8=\x0c\x8d\xbd'\x06\xcf\xef\x1d\x855\xf8\x07j\x97M\xa6VM2\xcfp", 0.00924400000000003)

T decrypt =>    Elapsed: 0.008960 seconds
Decrypted:      (b'emin and robert project, testing for speed', 0.008960499999999927)
------------------
```


EXPLORER
OPEN EDITORS
Encryption.py
dump.txt M
ENCRYPTION-TE...
__pycache__
.gitignore
dump.txt M
Encryption.py
LICENSE
README.md
Encryption.py
dump.txt M
dump.txt
Type: AES
Testing key: key0_16_bytes => m2G2hb*XVnC#&=:@
Plain text: emin and robert project, testing for speed
Encrypted: b"\x1e\x83\t\x0ft\xb8\xb9\x10\x01_\x1b\xb8u\xf6\xf0F4\x965\x18i\x91DZ\xf8Xx\x97'\xd0<Xc\x04\r\xec9\xefo^\x86\x9d"
Delta Time => 0.0006550999999999085s
Decrypted: emin and robert project, testing for speed
Delta Time => 0.00037980000000015224s
Type: DES Triple
Testing key: key0_16_bytes => m2G2hb*XVnC#&=:@
Plain text: emin and robert project, testing for speed
Encrypted: b'9\x90@\xa0\x124~e\xc1p! J\xab\xf0]\x1d1\xe8$\xb4\xbc\xf3\xb0\xe7\xf5m\xb30d\xa8\xb9e\x91\xae\xd7L_M\xcd\xbe"v5\xca\xa7
Delta Time => 0.0091821999999999918s
Decrypted: b'emin and robert project, testing for speed'
Delta Time => 0.0090466000000000016s
Type: AES
Testing key: key1_16_bytes => 2:[cNLKX89N#j9^+
Plain text: emin and robert project, testing for speed
Encrypted: b'\x1e\xc7\xad_ja\x15\xa3\xbf\x99[N\xb4\xf0\x96\x9e\xc3\x06N\x86\xe6/\xd2.\x948\xd75V\xc1\xb7\xd3\x04\x82y)\x14\x83\xbc\
Delta Time => 0.0003933000000004084s
Decrypted: emin and robert project, testing for speed
Delta Time => 0.00037200000000003897s
Type: DES Triple
Testing key: key1_16_bytes => 2:[cNLKX89N#j9^+
Plain text: emin and robert project, testing for speed
Encrypted: b'\xcc\xd5\xea\xd3\xbd\x0b\xa8\xcc\x8b\x00\x13Hc\x0f\\Y\x18\xf6\xbe\x1er1\xd2#\xdb5\x8d{y 8\x84\x18E?|r\x88\xceB\n\x04\x
Delta Time => 0.0090607999999999869s
Decrypted: b'emin and robert project, testing for speed'
Delta Time => 0.008928700000000012s
Type: AES
Testing key: key2_16_bytes => +D8eS'K#8*25(My$
Plain text: emin and robert project, testing for speed
Encrypted: b'2\x10\xb2\xbd\x9bX\x9b<e\xd8\xdan+5\xf6\xe9f\xd5?\xf4\xa9-\xc5\x7f\xbd\xea\xd4\x08Pn\xdc\xa8\xeb[\xd9\x8c\x9c\xd3\x8d\
Delta Time => 0.0003997000000000283s
Decrypted: emin and robert project, testing for speed
Delta Time => 0.0005039999999998379s
Type: DES Triple
Testing key: key2_16_bytes => +D8eS'K#8*25(My$

Bibliography

"Cryptography with Alice and Bob." *Word to the Wise*, 17 Sept. 2014, wordtothewise.com/2014/09/cryptography-alice-bob/.

Thakkar, Jay. "DES vs AES: Everything to Know About AES 256 and DES Encryption." *InfoSec Insights*, 20 Nov. 2020, sectigostore.com/blog/des-vs-aes-everything-to-know-about-aes-256-and-des-encryption/.