Encryption

Symmetric vs Asymmetric Encryptions

Asymmetric encryption holds one key that both the client and the server hold

Symmetric - For all a, b in X if a is related to b then b is related to a.

Asymmetric - For every a, b pair in X if a is related to b then b is not related to a.

Block vs Stream Encryption

Block Encryption- When the data being encrypted is placed into blocks of a declared size and padded to fill the room left available.

Stream Encryption- When the data being encrypted is in a one to one relation with with the output encrypted text.

Modes of Operation

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)

AES

The Basics

Advanced Encryption Standard (AES)

Background

- Encryption Type: Symmetric
- Original Name: Rijndael

Forms of AES include

- AES-128 (10 Rounds Keys)
- AES-192 (12 Rounds keys)
- AES-256 (14 Rounds Keys)

AES

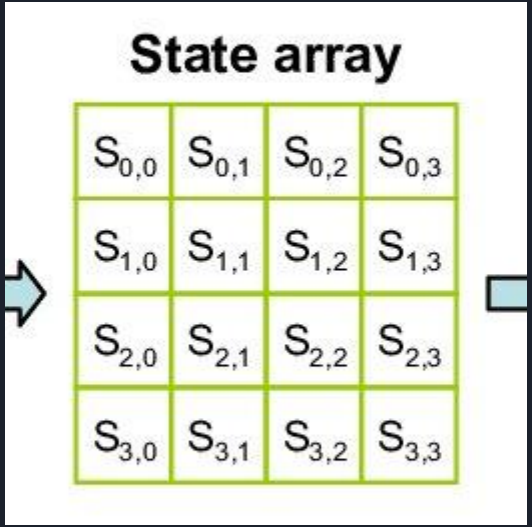
Encryption

State Array

- Derived from block data

- Holds state of encryption throughout the process

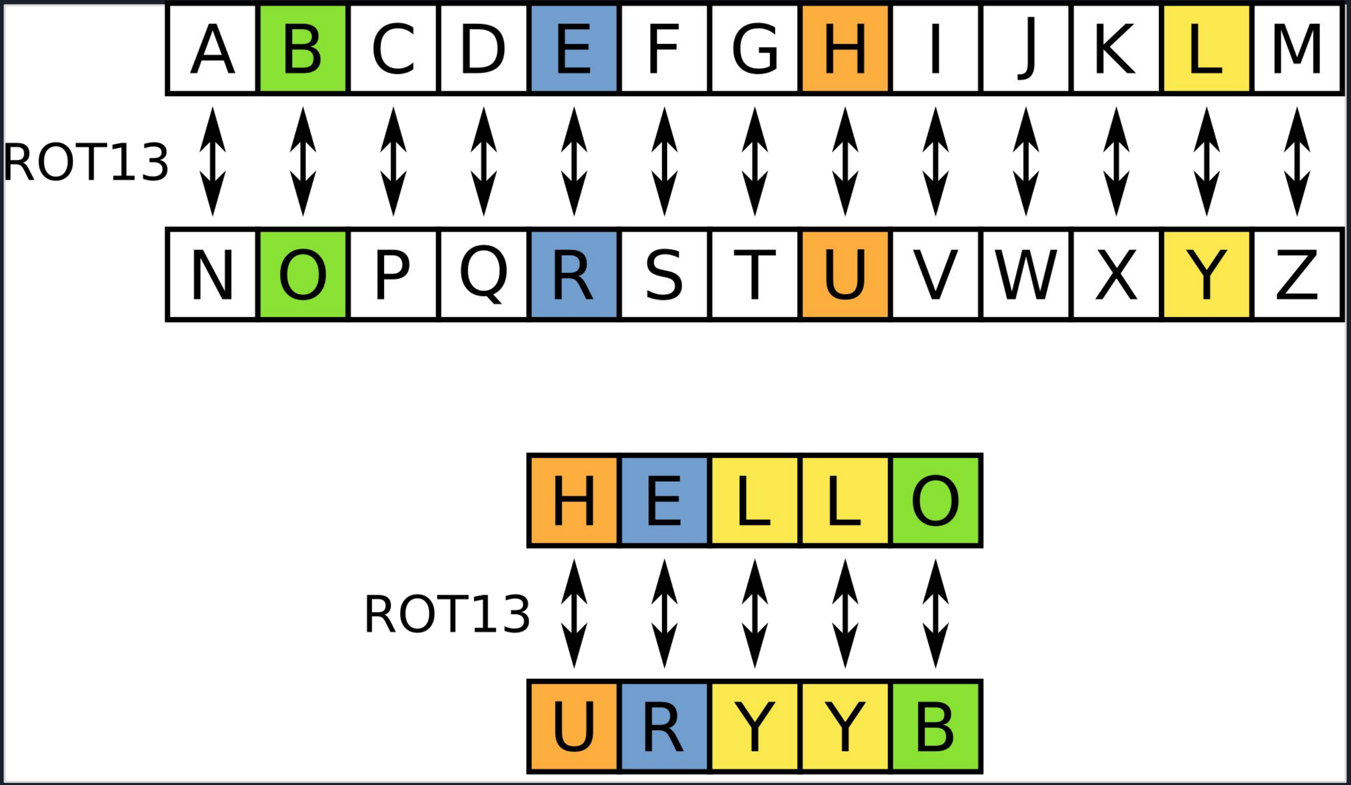
- Center focus of the encryption



State array

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Substitution box (S-Box)



ROT13

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

ROT13

H	E	L	L	O
U	R	Y	Y	B

Round constant (Rcon)

1 -> 2

2 -> 4

3 -> 8

4 -> 16

5 -> 32

6 -> 64

7 -> 128

8 -> 27

9 -> 54

10 -> 108

Round Key

- X keys that are derived from the original key, the first round being the key itself,

- Each Key is derived from the last

- Each key contains 4 32 bits words (W)

Formulas:

- R(x) =

x rotated right 8 bits

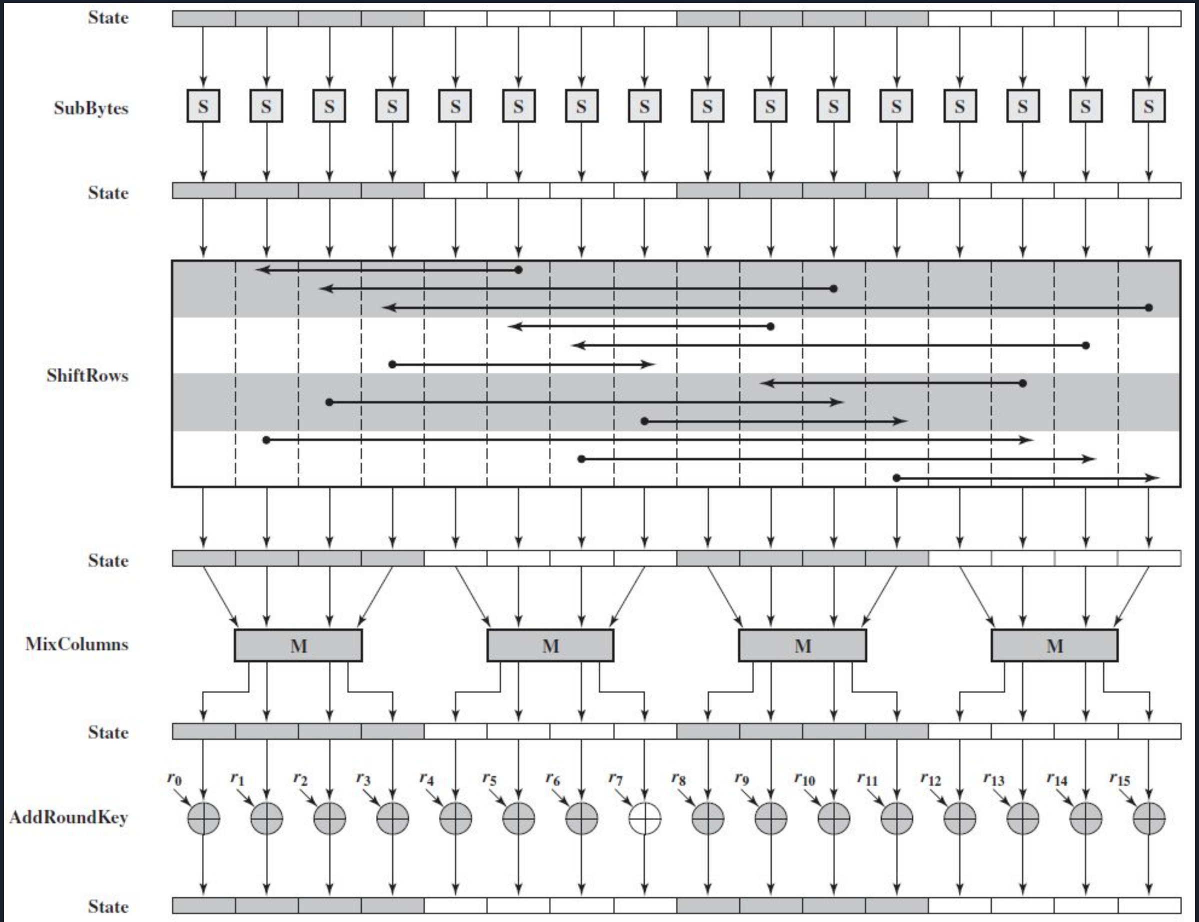
- Key(i):W(0)=

Key(i-1):W(0) XOR R(Key(i-1):W3) XOR Rcon[i]

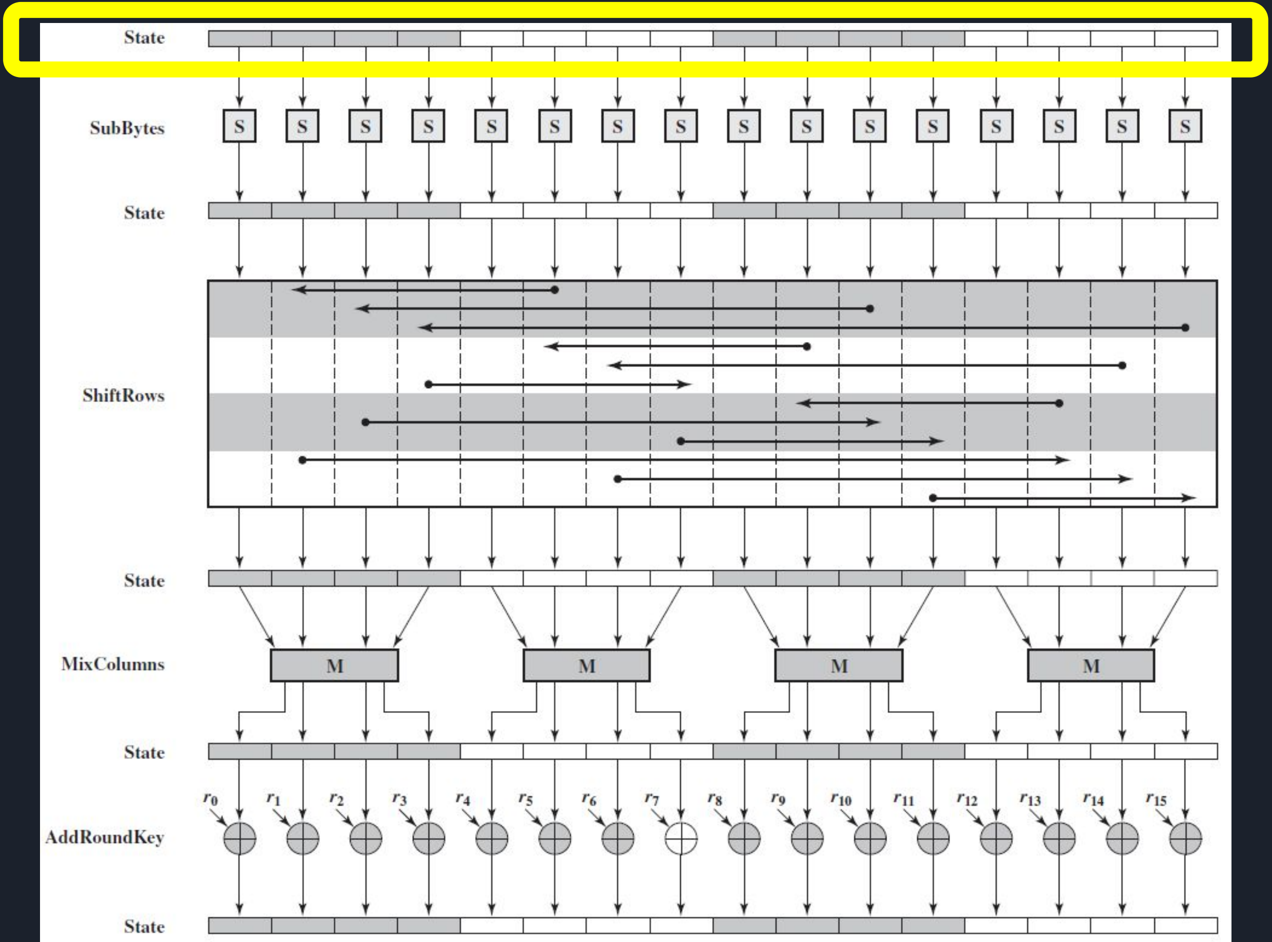
- Key(i): W(i) =

Key(i-1):W(i) XOR Key(i):W(i-1)

The Process

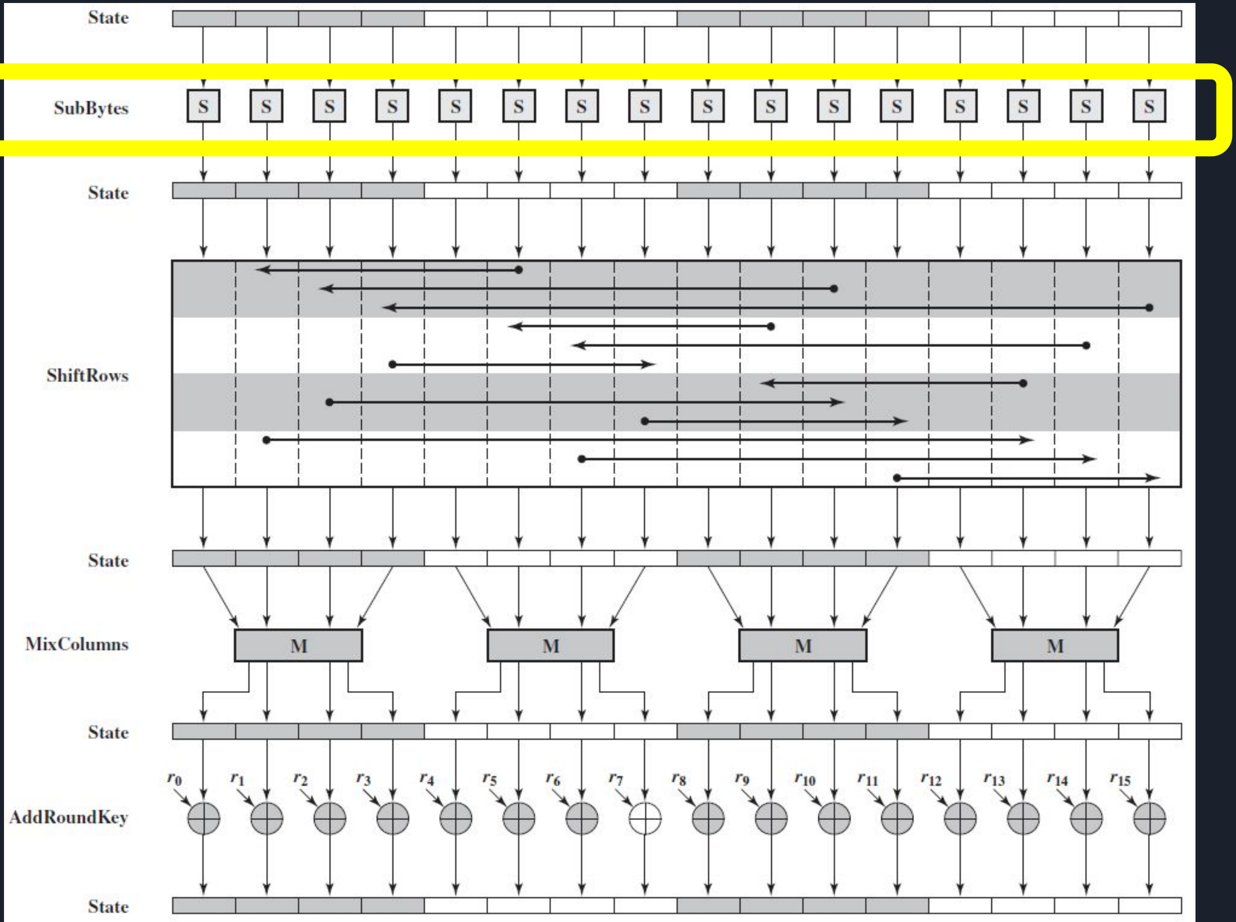

State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

The Process

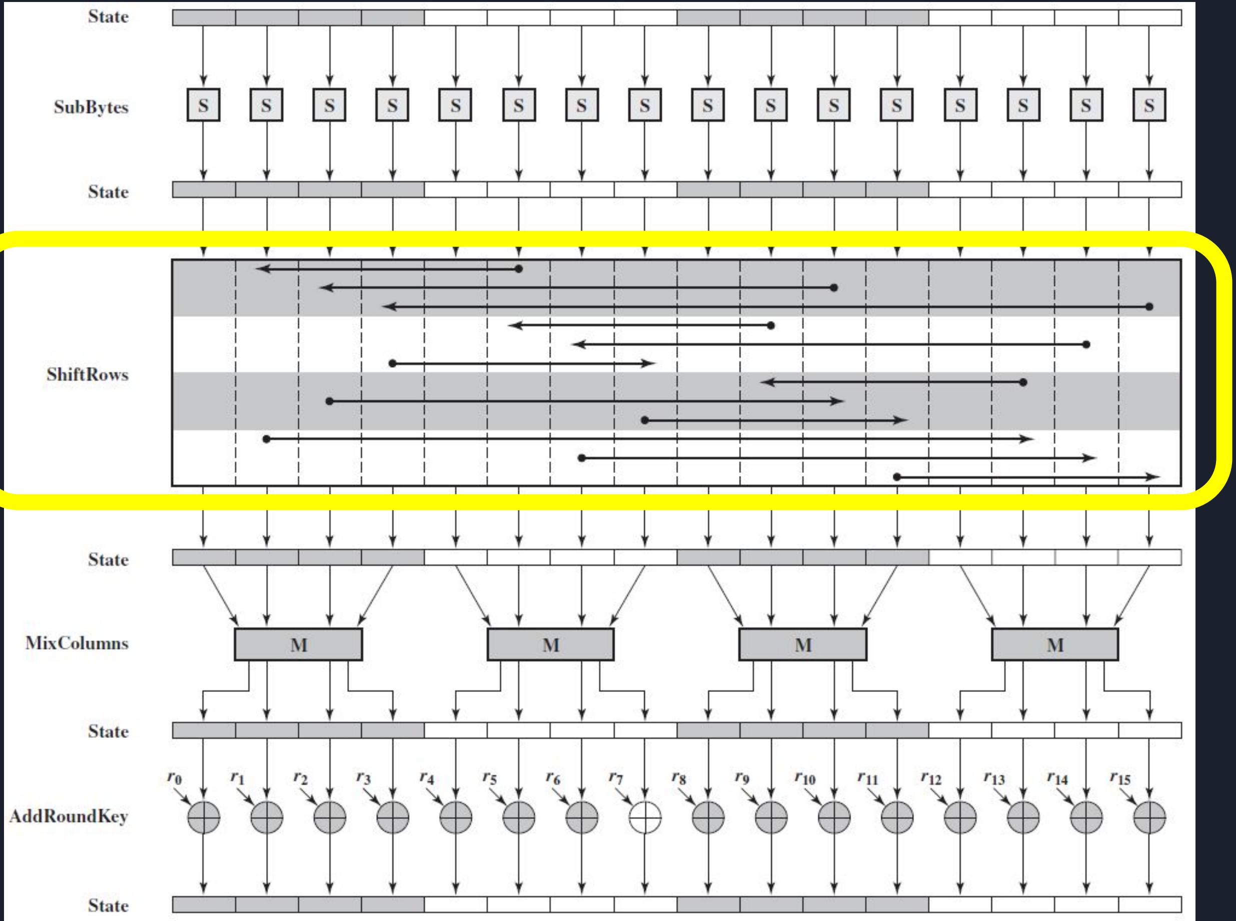


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

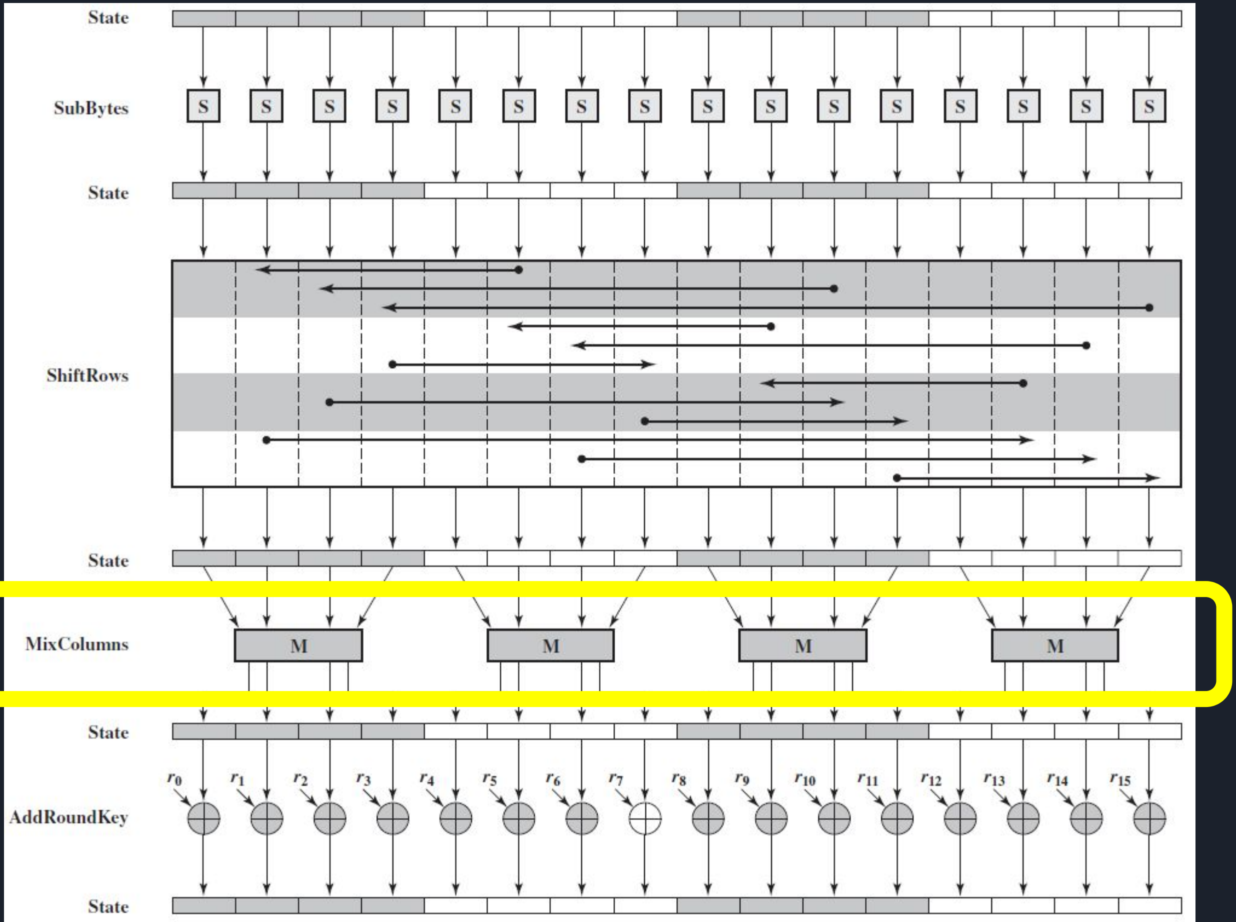
The Process


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0
r_1
r_2
r_3
r_4
r_5
r_6
r_7
r_8
r_9
r_{10}
r_{11}
r_{12}
r_{13}
r_{14}
r_{15}
State

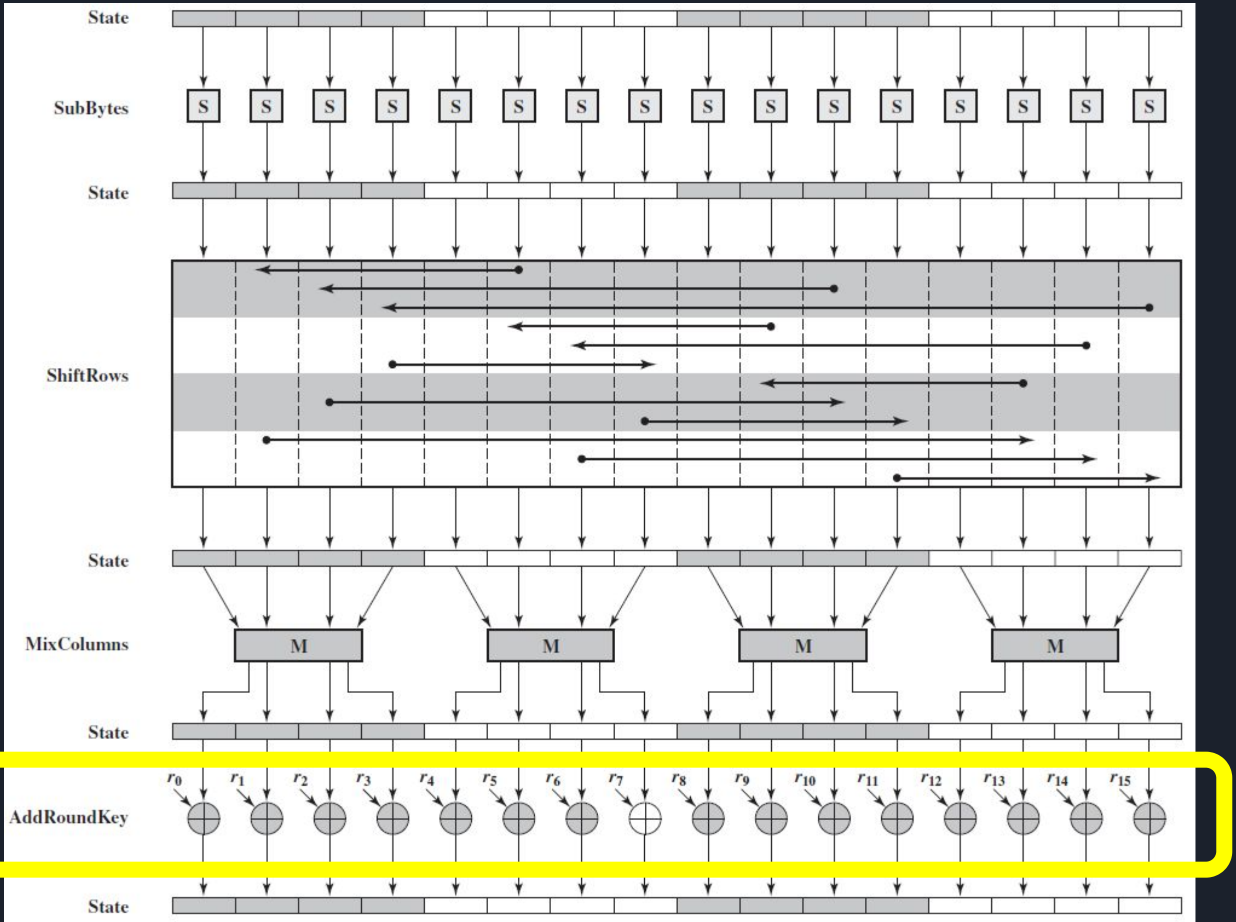
The Process

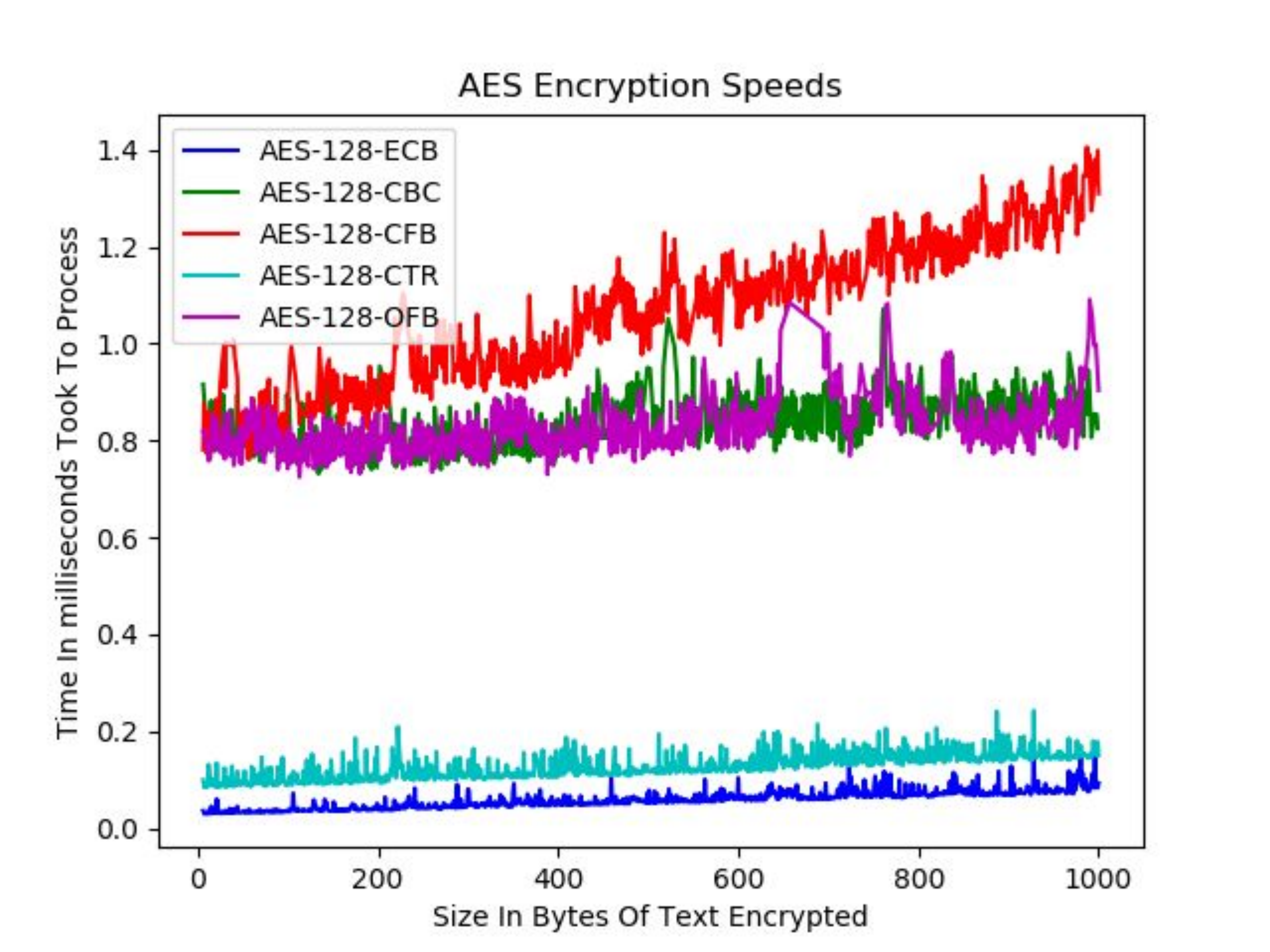

State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
AddRoundKey
State

The Process


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
AddRoundKey
State

The Process


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State


AES Encryption Speeds
AES-128-ECB
AES-128-CBC
AES-128-CFB
AES-128-CTR
AES-128-OFB
Time In milliseconds Took To Process
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
0
200
400
600
800
1000
Size In Bytes Of Text Encrypted

AES

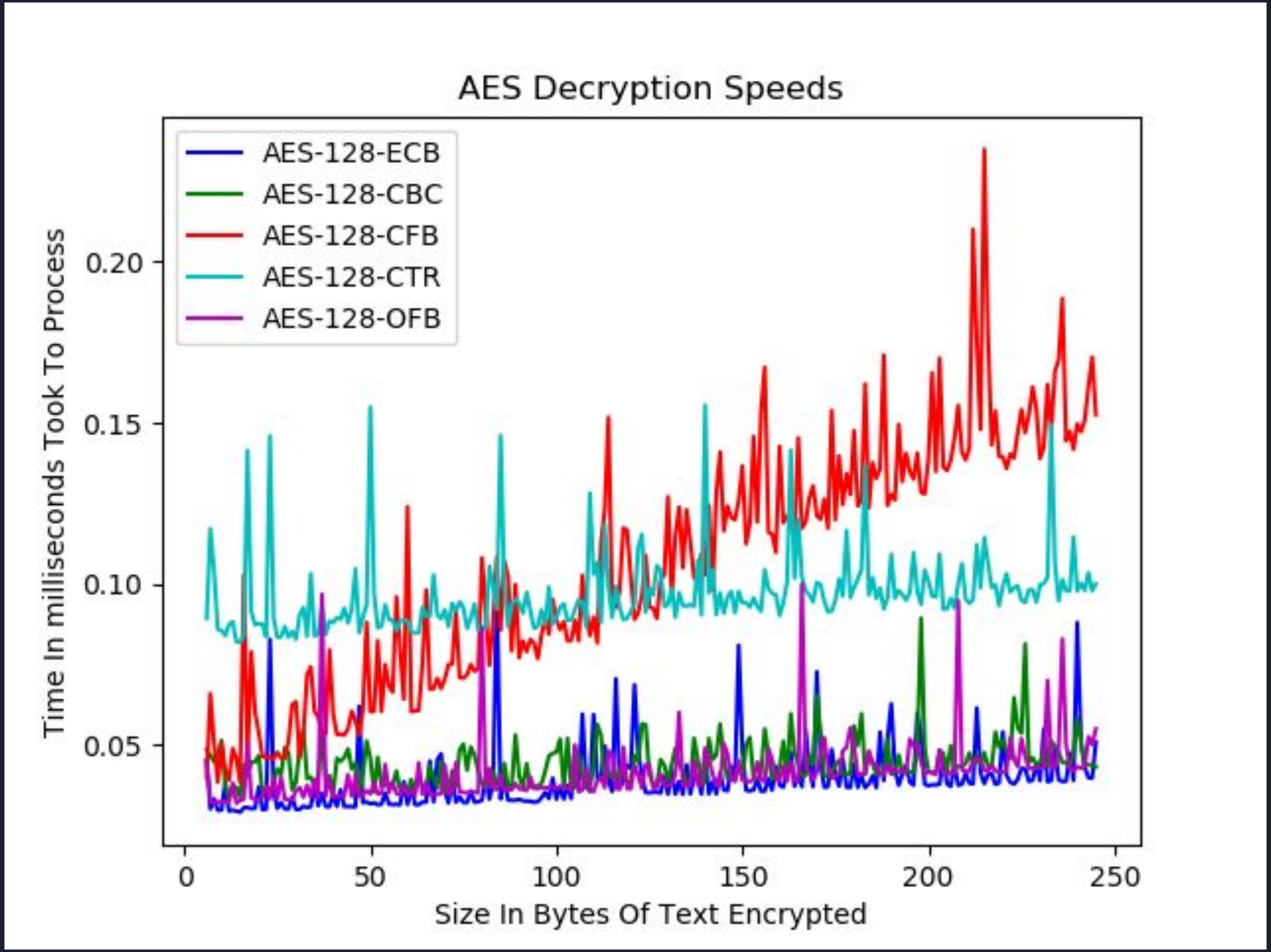
Decryption

Advanced Encryption Standard Decryption

Methods/ Functions Required

- Inverse Substitute Bytes
- Inverse Shift Rows
- Inverse Mix Columns

Apply all the rules in reverse, since everything is XORed we can use XOR to return to the previous state


AES Decryption Speeds
AES-128-ECB
AES-128-CBC
AES-128-CFB
AES-128-CTR
AES-128-OFB
Time In milliseconds Took To Process
0.05
0.10
0.15
0.20
0
50
100
150
200
250
Size In Bytes Of Text Encrypted

RSA

The Basics

Rivest, Shamir, Adleman (RSA)

Background

- Named after its founders;
  - Ron **R**ivest,
  - Adi **S**hamir
  - Leonard **A**dlema

Important Details:

- Encryption Type: Asymmetric
- Stream Encryption
- Main focus of RSA is in the modulus and the exponent
- Math oriented
- Limited to 245 bytes at a time

Key Generation - How does it work

Private Key:

1. Two prime numbers are picked at random, p and q
2. The modulus is then found
3. Length is founda
4. List all integers from 2 to length
5. Choose one that is a coprime with both the length and the modulus
6. That number is now the exponent

Equations:

modulus = p * q

Length(Euler's Totient) = (q - 1) * (p - 1)

Key Generation - How does it work

Public Key:

1. Retrieve the private key’s modulus and exponent
2. Using the exponent from the private key we can solve for d, there will be multiple answers for this where the range is infinit. Any of the possibilities may be chosen.
3. Choose one at random, at that becomes the exponent
4. The modulus will match that of the private key’s

The Rule:

(D * exponent) % length = 1

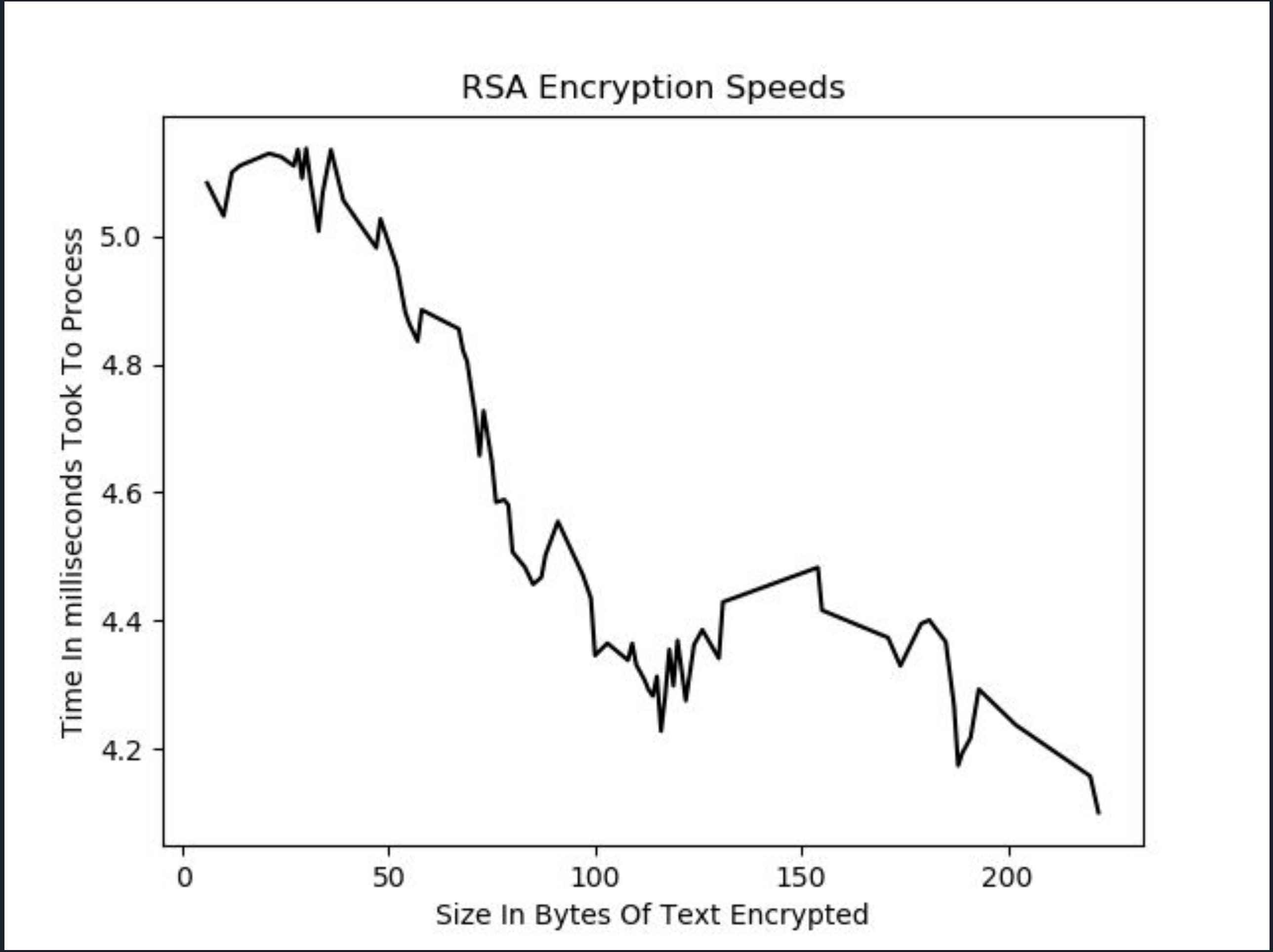
RSA Encryption

1. The public key is obtained

2. Each byte(b) is then put into the following equation where *e* is its encrypted value

   b^(exponent) % modulus = *e*

3. All the bytes are then placed together again and form a new byte array


RSA Encryption Speeds
Time In milliseconds Took To Process
5.0
4.8
4.6
4.4
4.2
0
50
100
150
200
Size In Bytes Of Text Encrypted

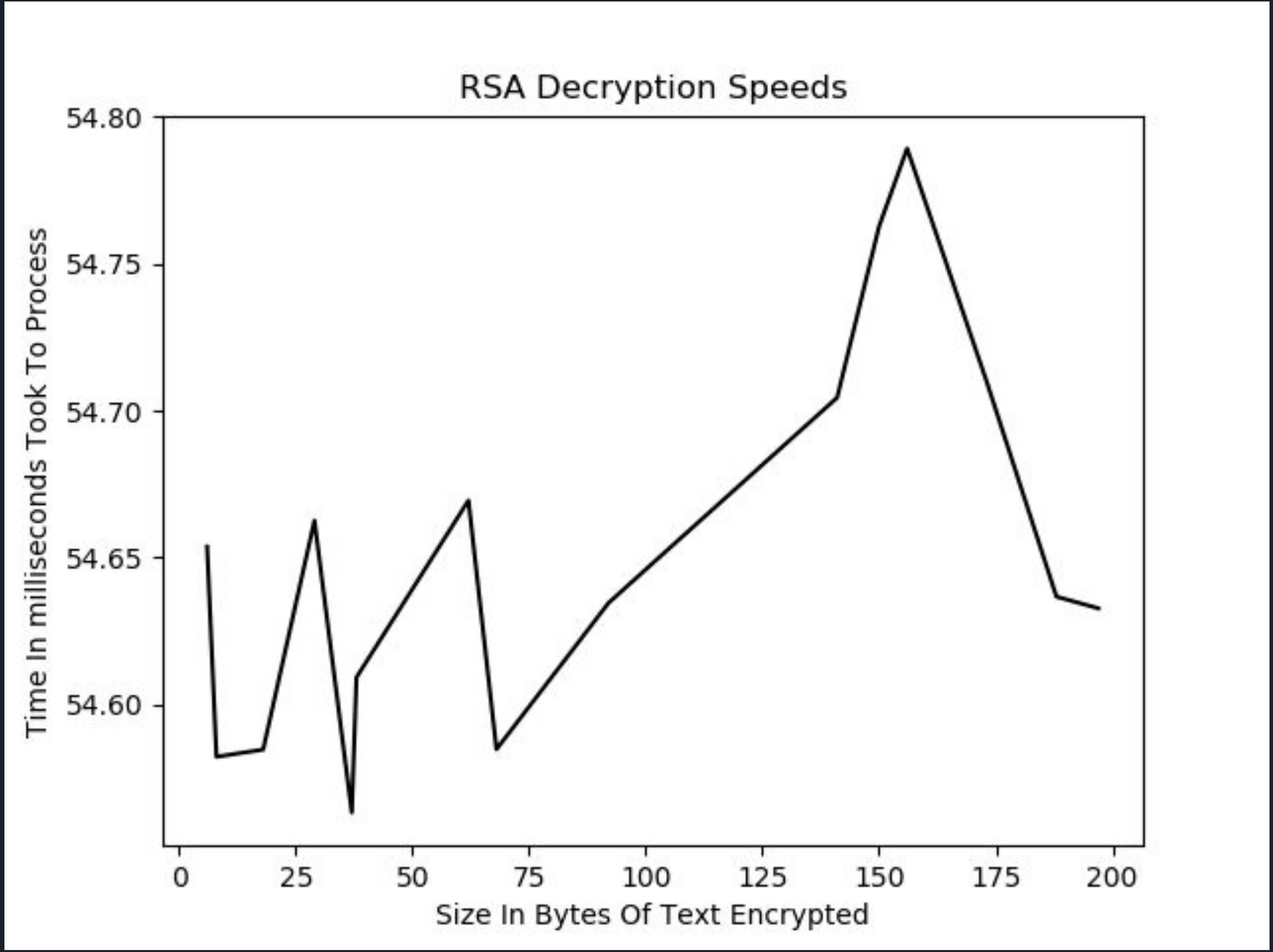
RSA Decryption

1. The private key is obtained
2. The bytes(*b*) given in the encrypted text are put through the following equation

   just as before, where *d* is the decrypted byte

   b^(exponent) % modulus = d

3. All the bytes are then placed together again and form a new byte array that can then be turned turned into a decrypted string

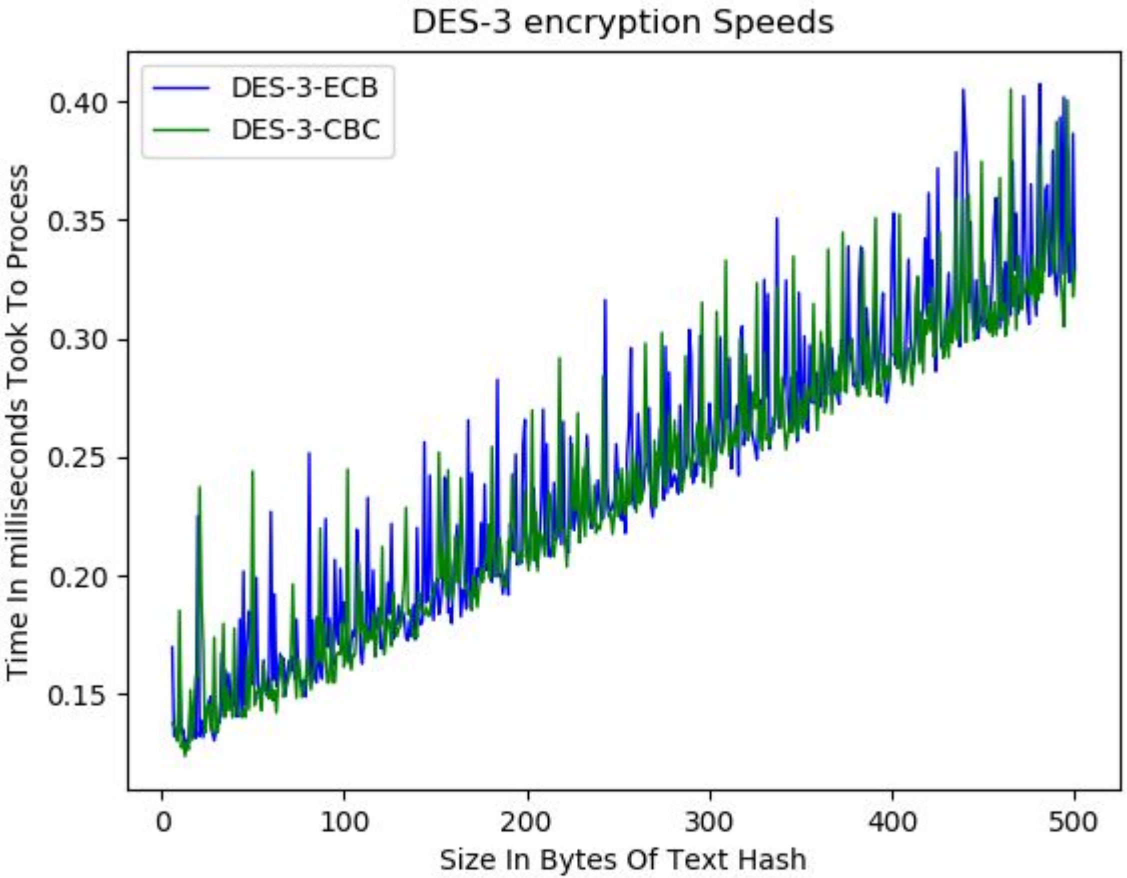

RSA Decryption Speeds
Time In milliseconds Took To Process
54.80
54.75
54.70
54.65
54.60
0
25
50
75
100
125
150
175
200
Size In Bytes Of Text Encrypted

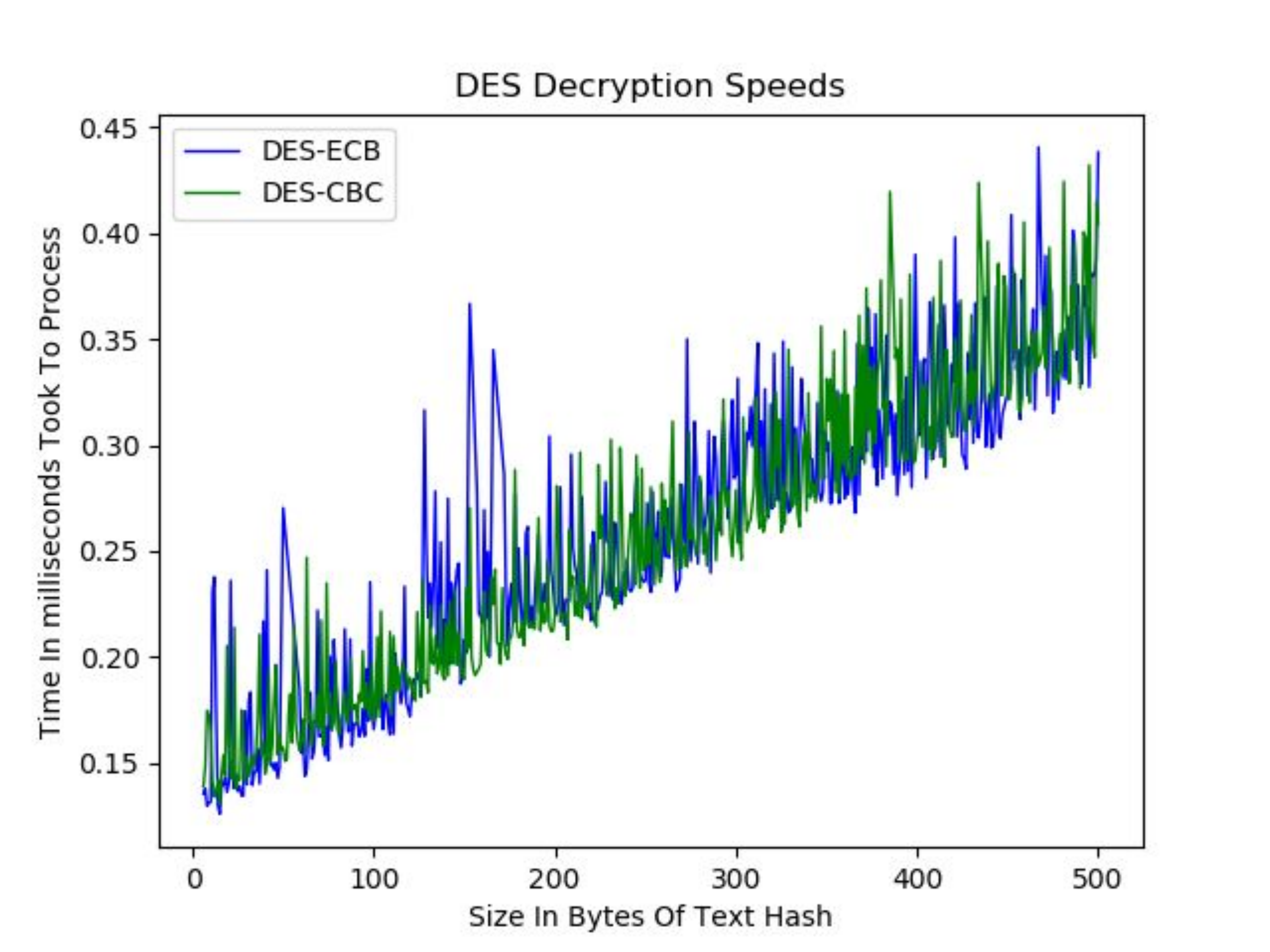
Data Encryption Standard

- Outdated
- Key with the size of 64 bits
- 8 of the bits from the key are reserved and unused during encryption, due to this DES is considered to have 56 bit keys
- Considered easy to break using a brute force attack

Triple Data Encryption Standard

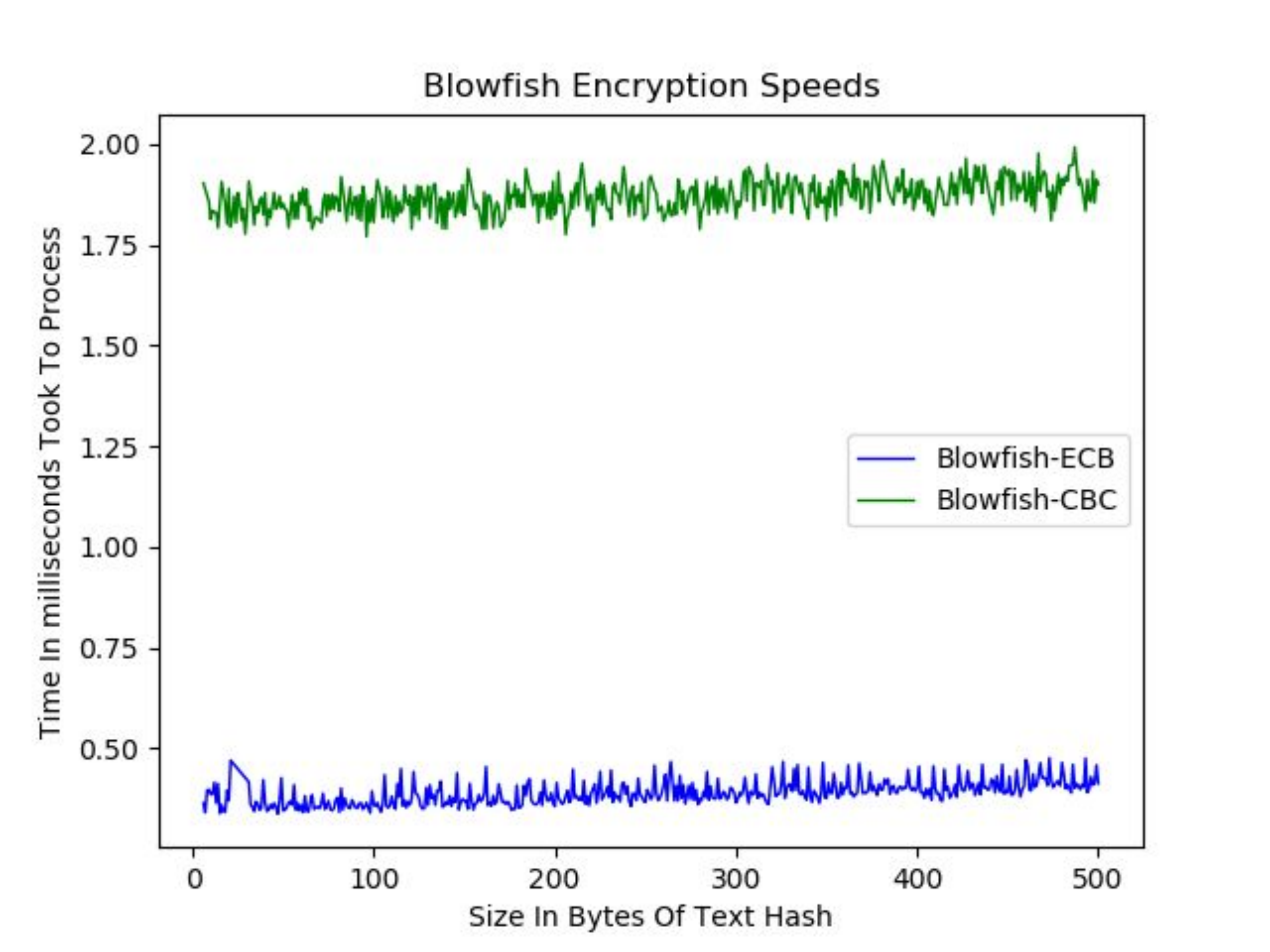
- The same algorithm that Single Data Encryption Standard uses
- 3 unique keys adding up to a total of 168-bits for a key
- Saved DES from being removed from the eyes of the world

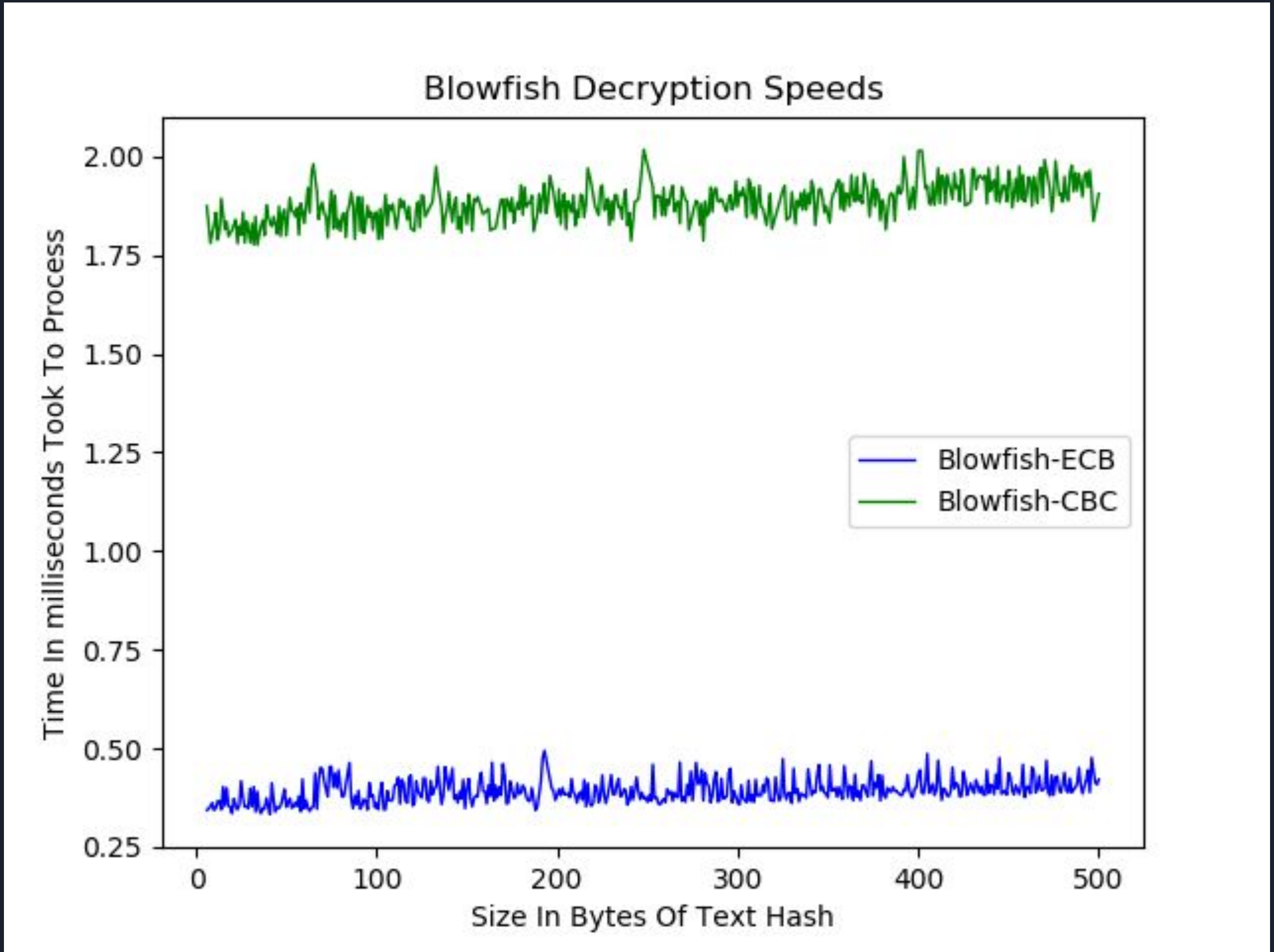

DES-3 encryption Speeds
DES-3-ECB
DES-3-CBC
Time In milliseconds Took To Process
0.40
0.35
0.30
0.25
0.20
0.15
0
100
200
300
400
500
Size In Bytes Of Text Hash


DES Decryption Speeds
DES-ECB
DES-CBC
Time In milliseconds Took To Process
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0
100
200
300
400
500
Size In Bytes Of Text Hash

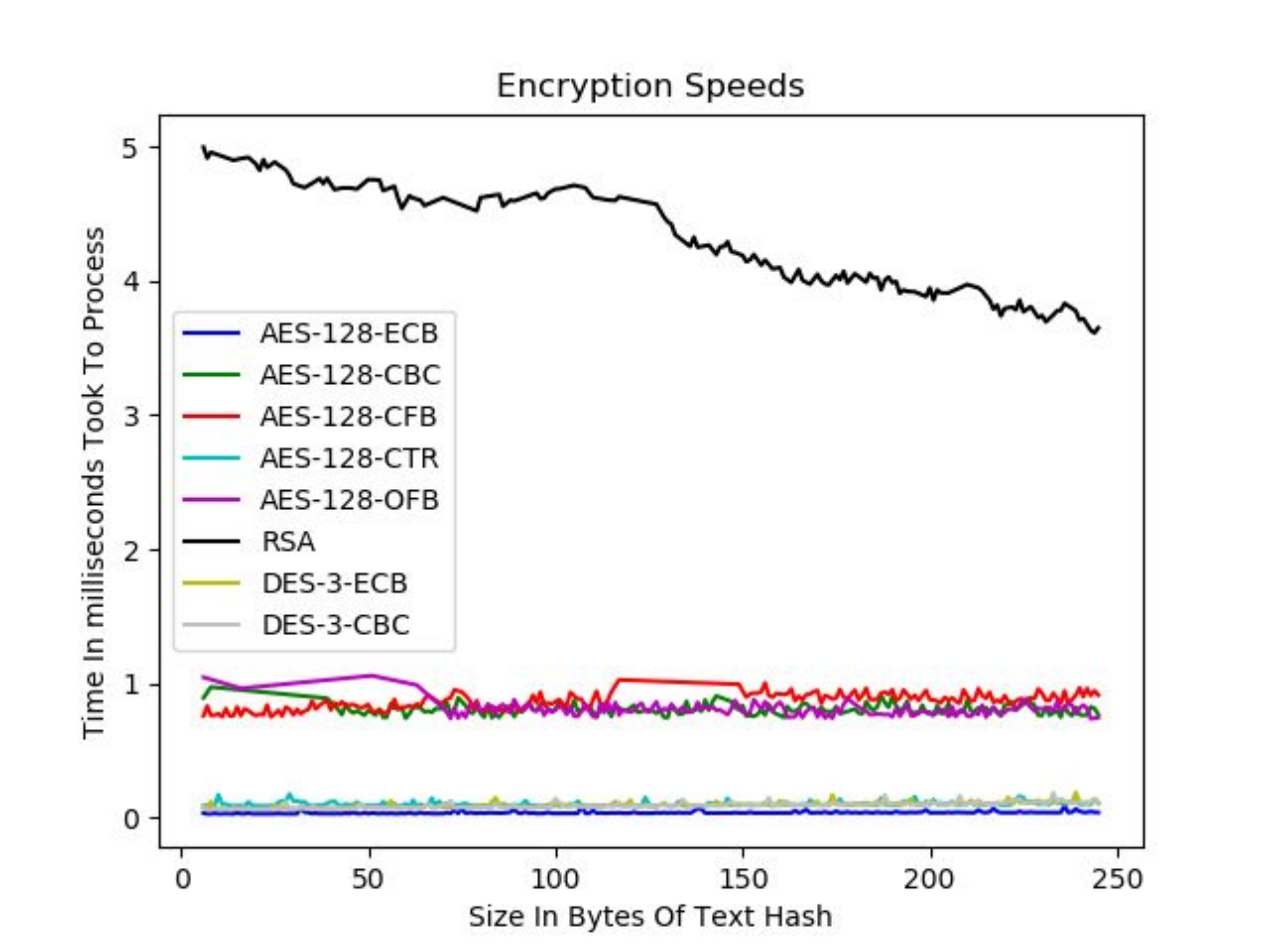
Blowfish Encryption

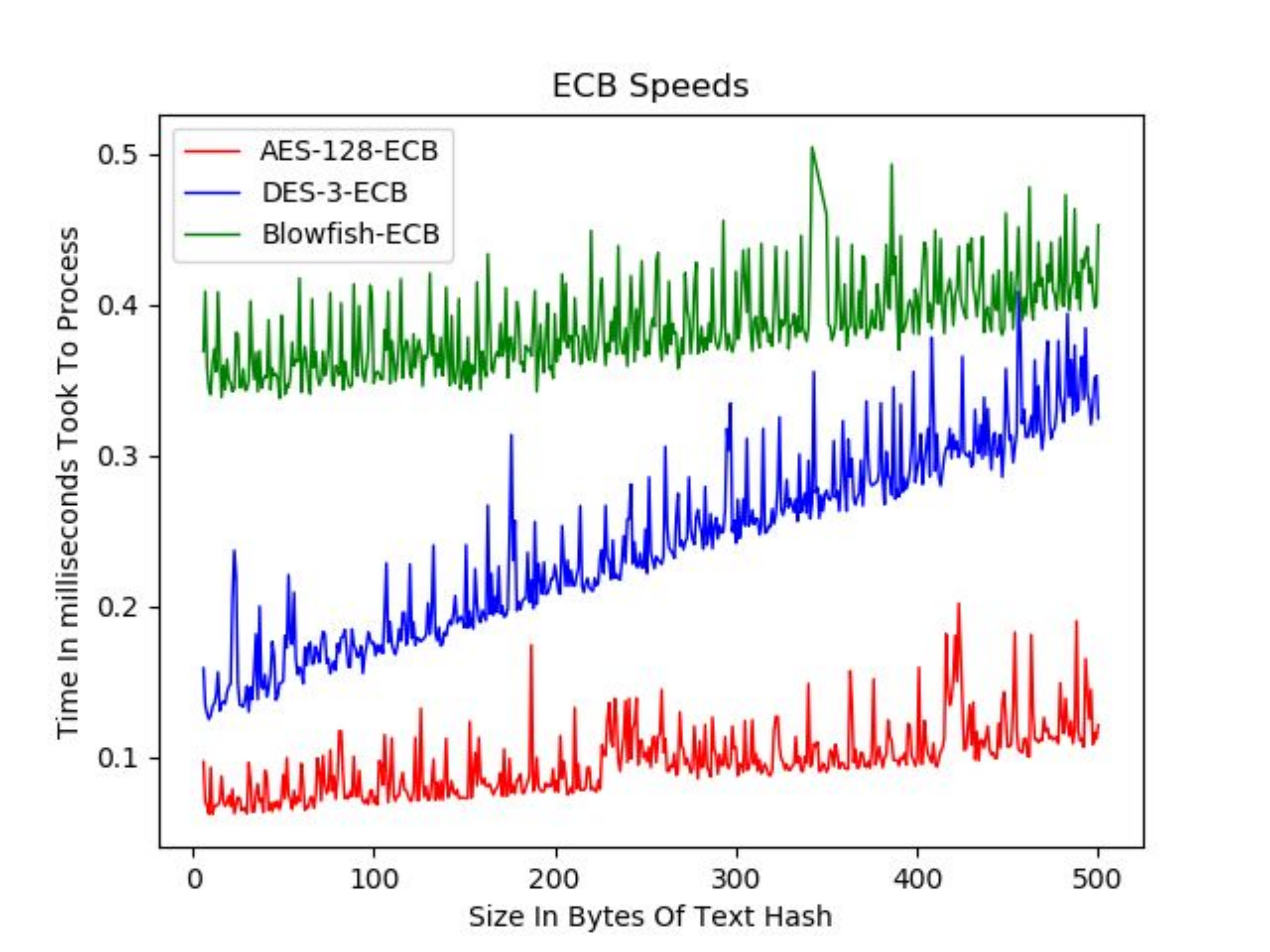
- Said to be the fastest algorithm, however it all depends on what mode is used at the time of encryption
- Discovered in 1993 in an attempt to replace DES
- Rated inferior to AES

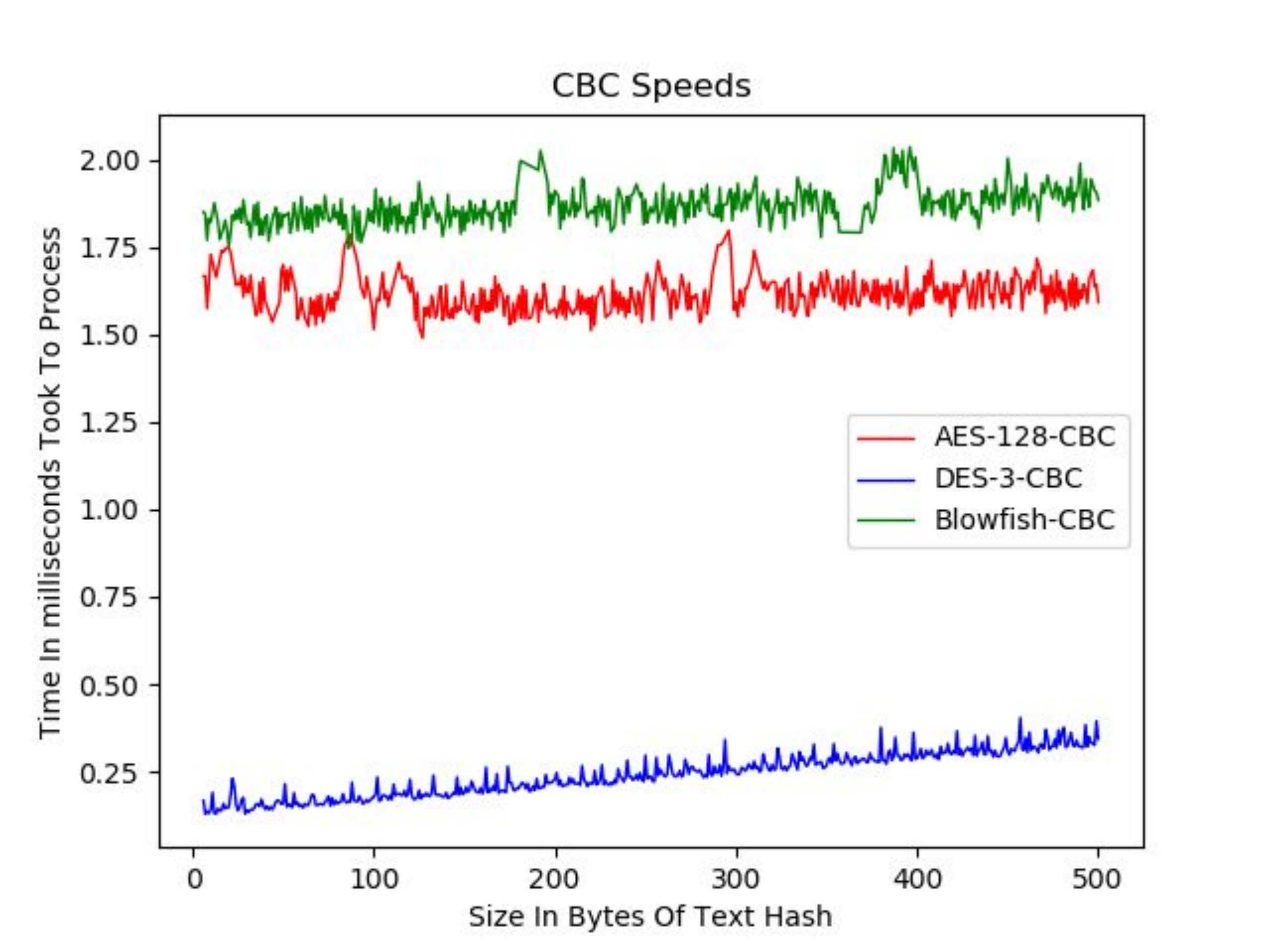

Blowfish Encryption Speeds
Time In milliseconds Took To Process
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0
100
200
300
400
500
Size In Bytes Of Text Hash
Blowfish-ECB
Blowfish-CBC


Blowfish Decryption Speeds
Time In milliseconds Took To Process
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0
100
200
300
400
500
Size In Bytes Of Text Hash
Blowfish-ECB
Blowfish-CBC

Comparing Encryption Method speeds


Encryption Speeds
Time In milliseconds Took To Process
5
4
3
2
1
0
0
50
100
150
200
250
Size In Bytes Of Text Hash
AES-128-ECB
AES-128-CBC
AES-128-CFB
AES-128-CTR
AES-128-OFB
RSA
DES-3-ECB
DES-3-CBC

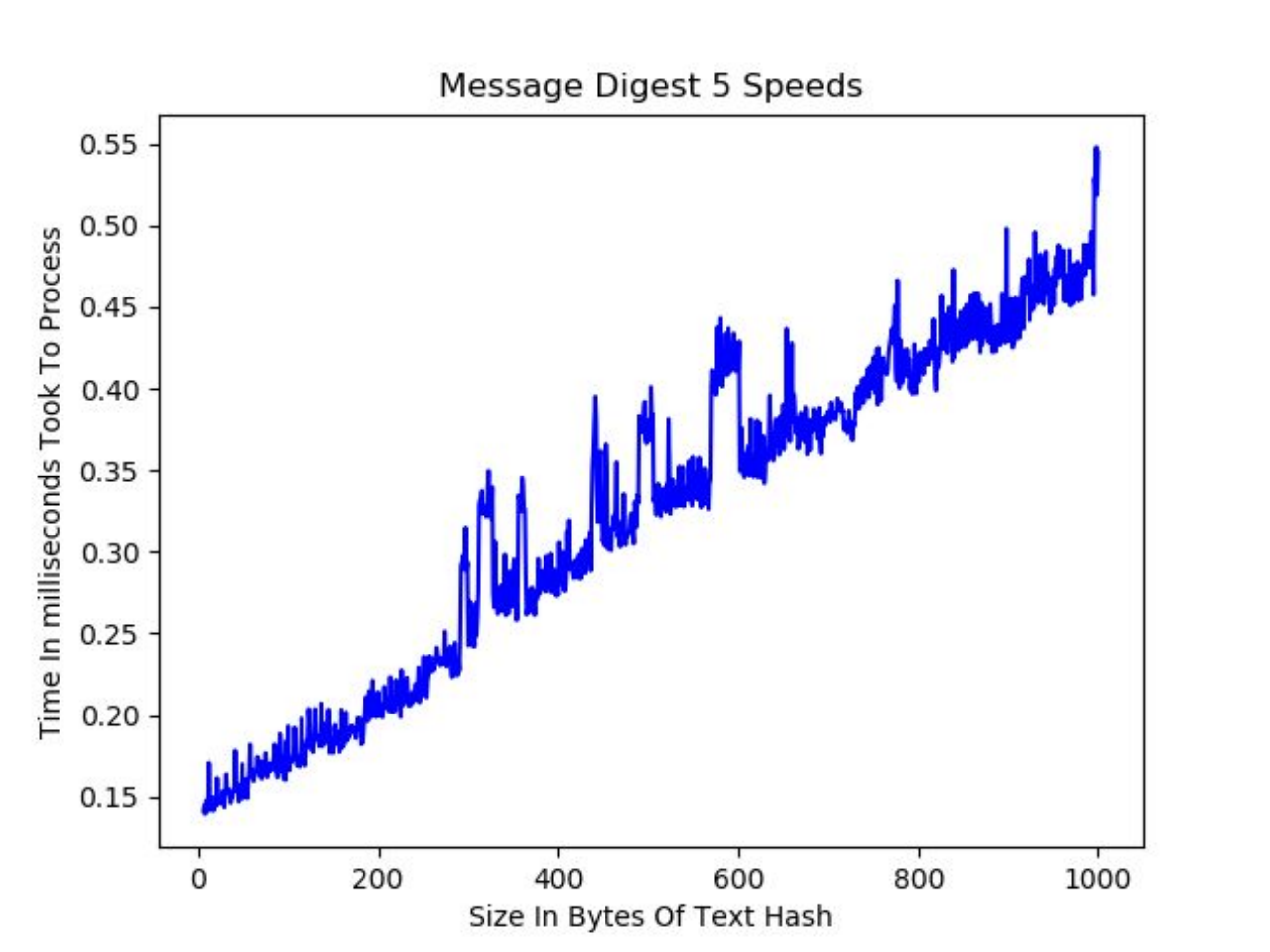

ECB Speeds
AES-128-ECB
DES-3-ECB
Blowfish-ECB
Time In milliseconds Took To Process
0.1
0.2
0.3
0.4
0.5
0
100
200
300
400
500
Size In Bytes Of Text Hash


CBC Speeds
Time In milliseconds Took To Process
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0
100
200
300
400
500
Size In Bytes Of Text Hash
AES-128-CBC
DES-3-CBC
Blowfish-CBC

Hashing

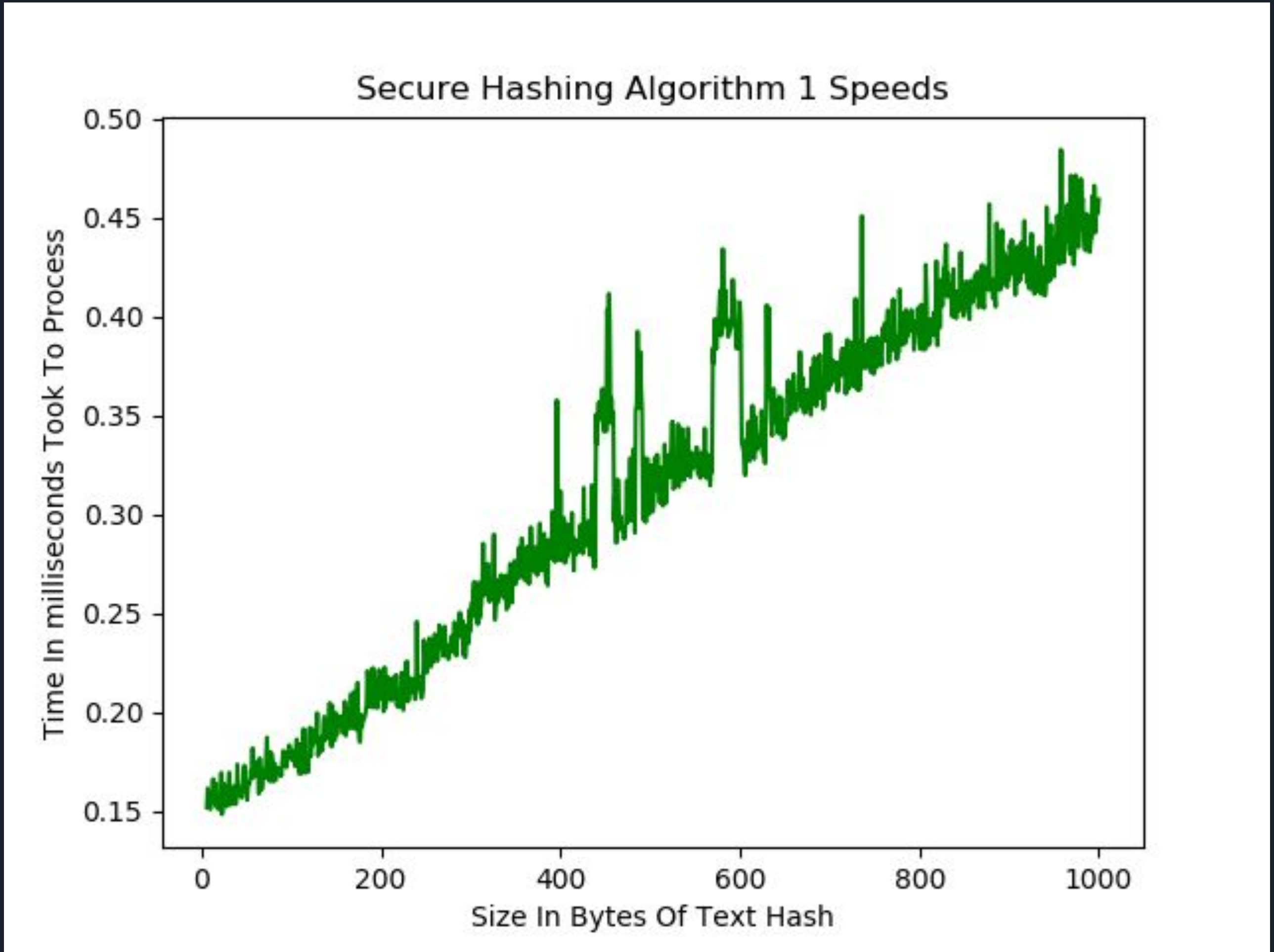
Message Digest

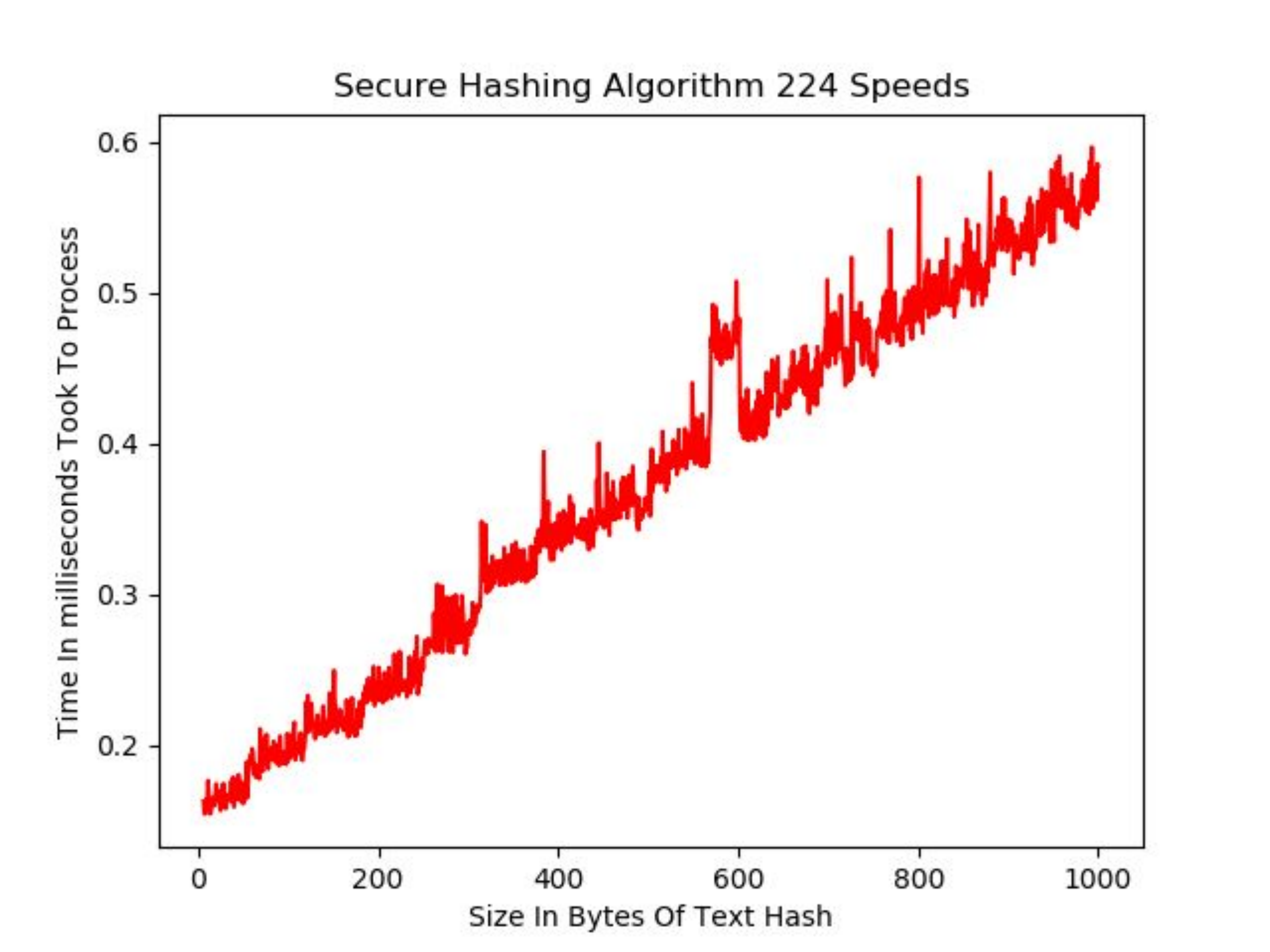
- Output: 128 bits
- Breaks words down into blocks
- Designed by Rivest, who also played a role in creating RSA

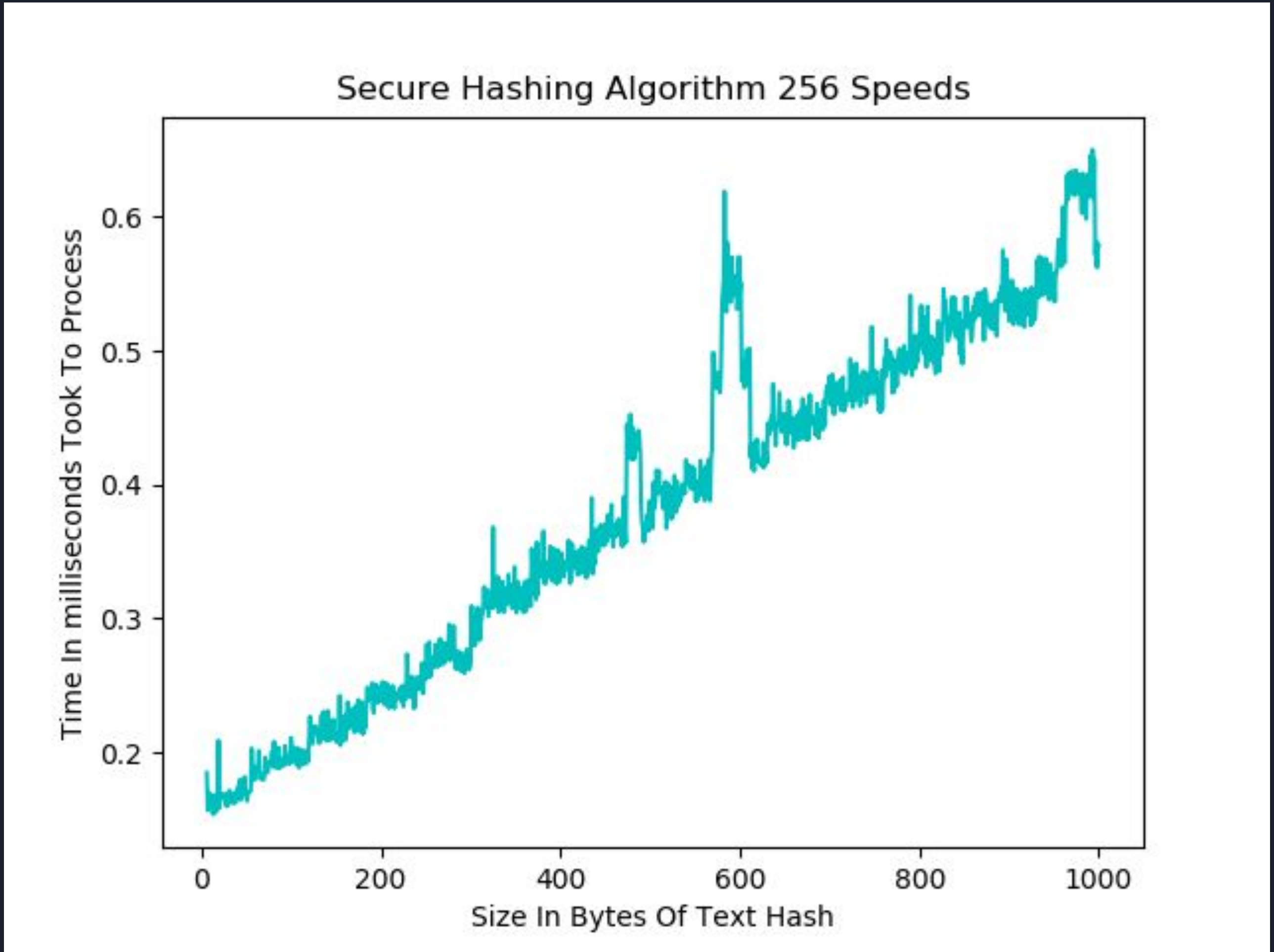

Message Digest 5 Speeds
Time In milliseconds Took To Process
0.55
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0
200
400
600
800
1000
Size In Bytes Of Text Hash

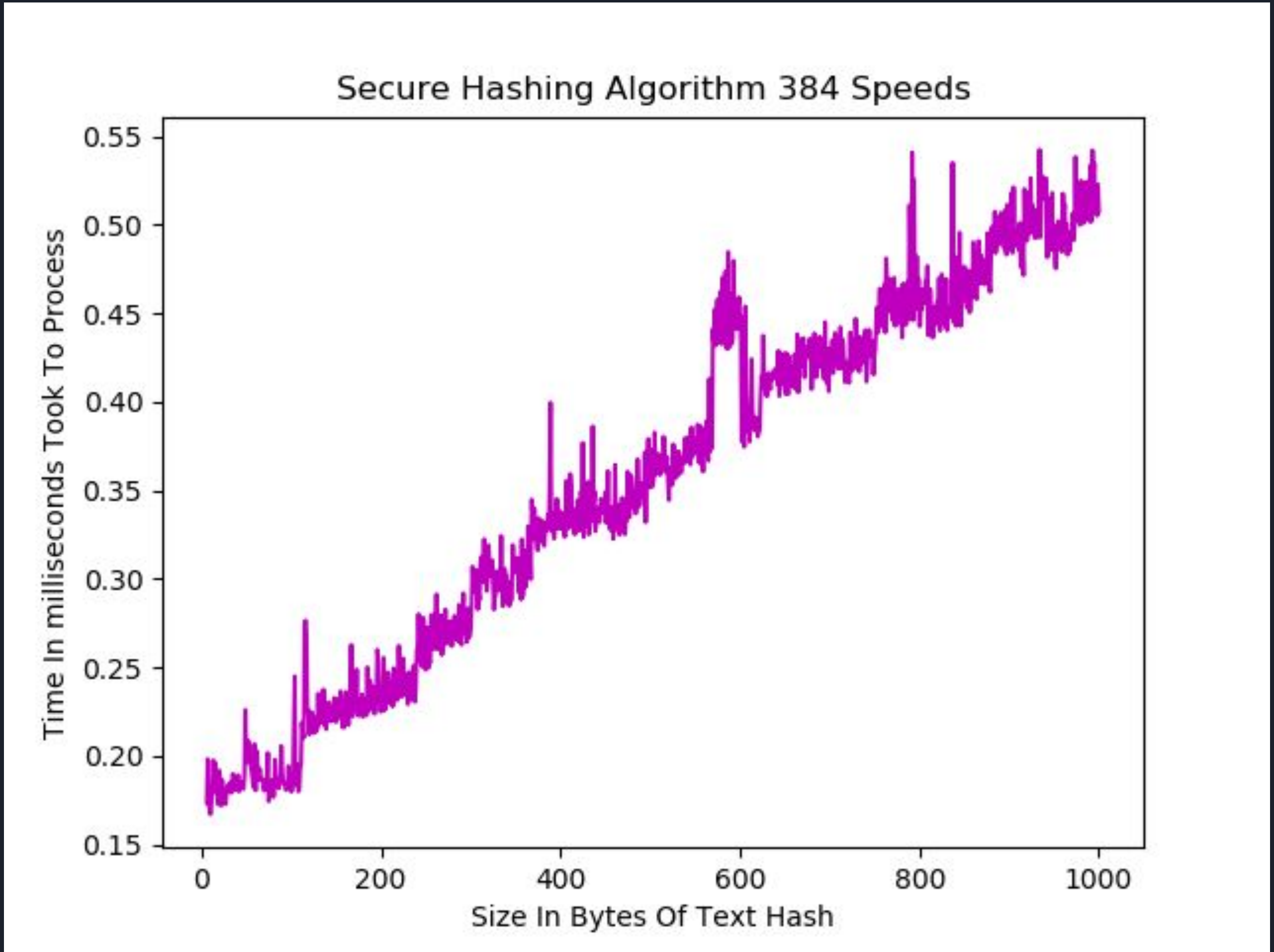
Secure Hashing Algorithms

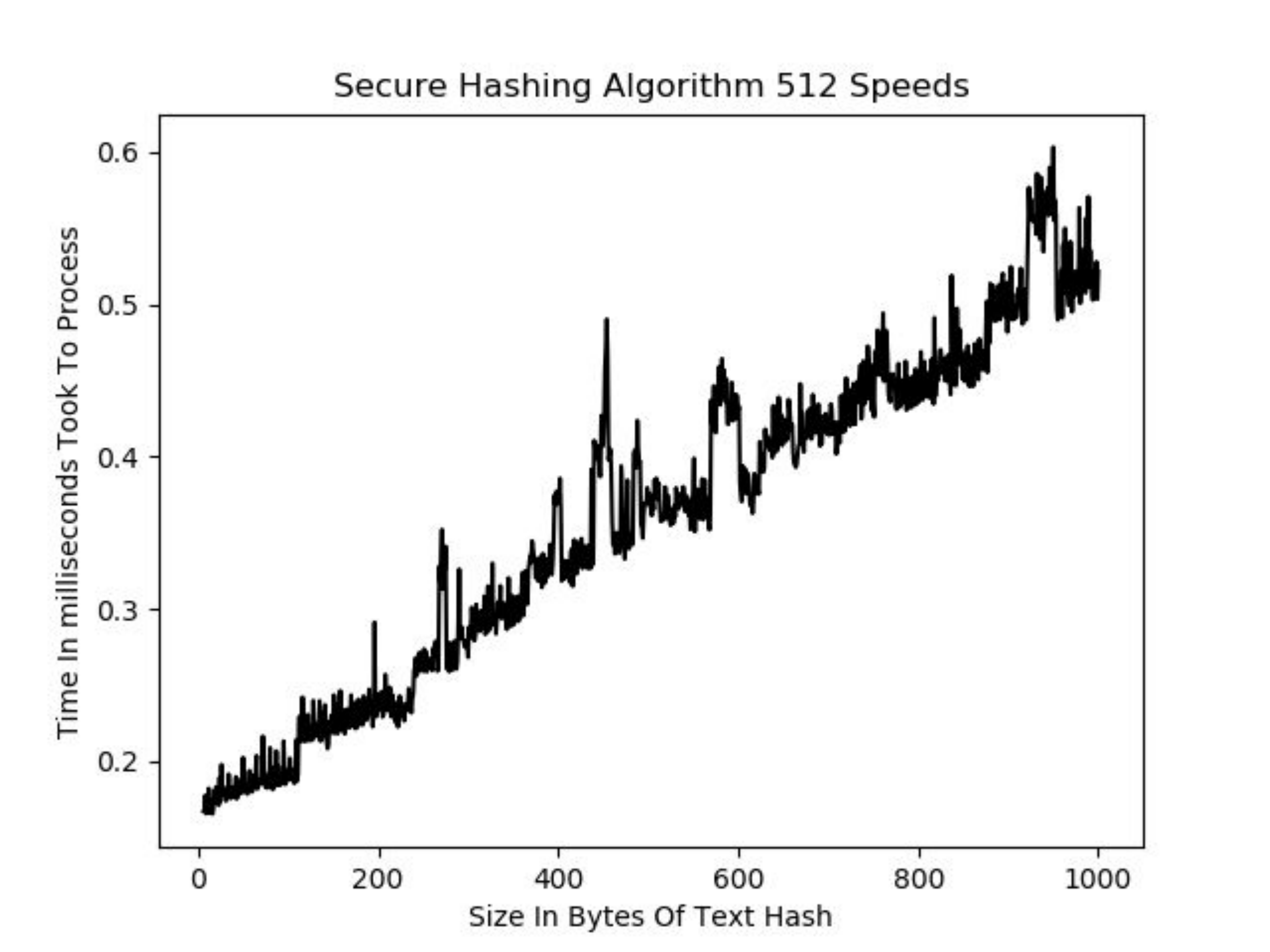
- Works in the form of blocks
- Sha Forms are broken into groups called SHA-0, SHA-1, SHA-2, SHA-3
  - SHA-0 contains only SHA-0
  - SHA-1 contains only SHA-1
  - SHA-2 contains SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
  - SHA-3 contains SHA-224, SHA-256, SHA-384, SHA-512, SHAKE128, SHAKE256


Secure Hashing Algorithm 1 Speeds
Time In milliseconds Took To Process
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0
200
400
600
800
1000
Size In Bytes Of Text Hash


Secure Hashing Algorithm 224 Speeds
Time In milliseconds Took To Process
0.6
0.5
0.4
0.3
0.2
0
200
400
600
800
1000
Size In Bytes Of Text Hash


Secure Hashing Algorithm 256 Speeds
Time In milliseconds Took To Process
0.2
0.3
0.4
0.5
0.6
0
200
400
600
800
1000
Size In Bytes Of Text Hash


Secure Hashing Algorithm 384 Speeds
Time In milliseconds Took To Process
0.55
0.50
0.45
0.40
0.35
0.30
0.25
0.20
0.15
0
200
400
600
800
1000
Size In Bytes Of Text Hash


Secure Hashing Algorithm 512 Speeds
Time In milliseconds Took To Process
0.2
0.3
0.4
0.5
0.6
0
200
400
600
800
1000
Size In Bytes Of Text Hash