Network Security

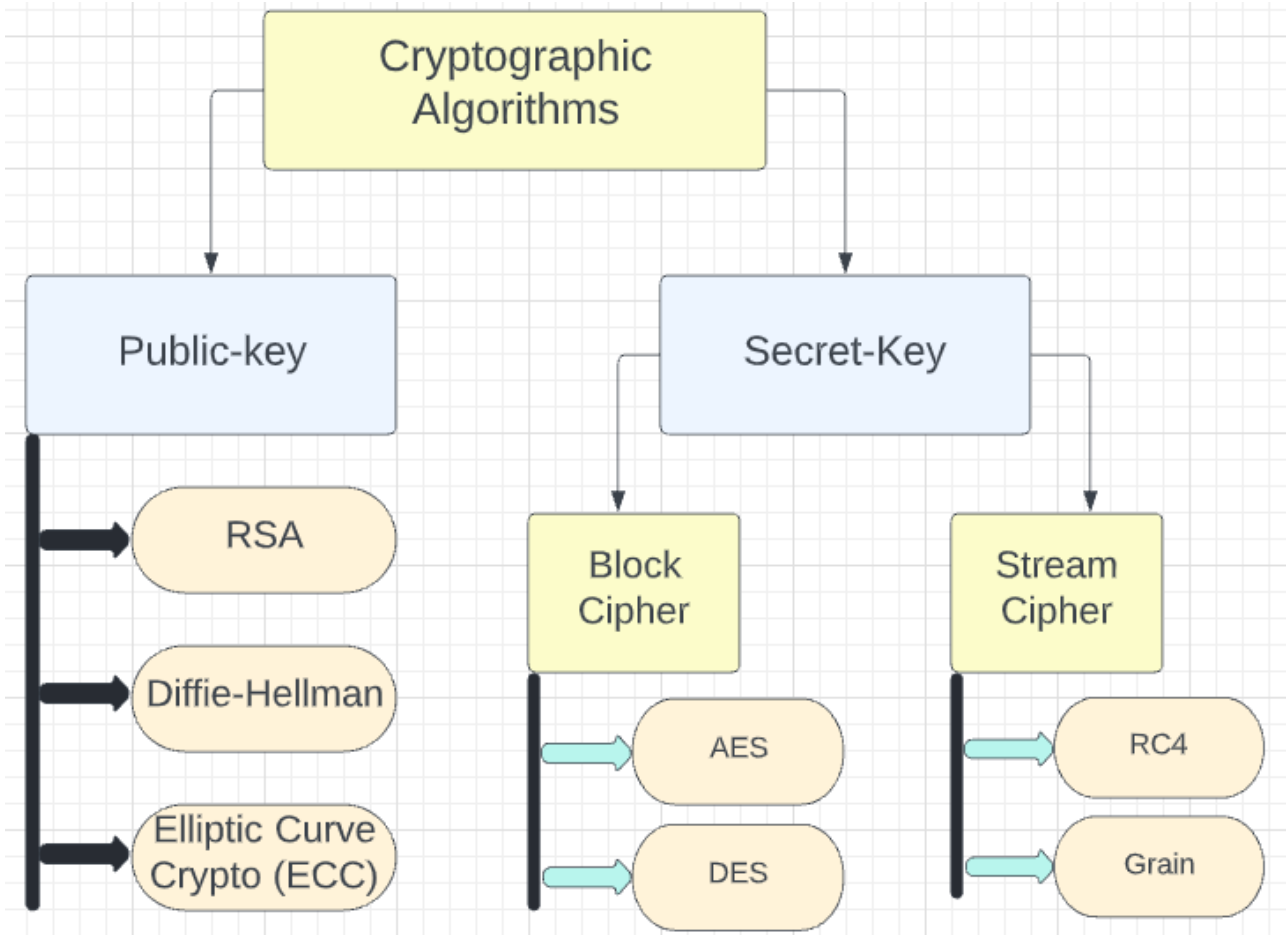
Performance Comparison of the state of art Block and Stream ciphers over TCP/UDP protocols for different types of wired/wireless networks, and applications.

By Talha Abdullah

Project Goals and Objectives

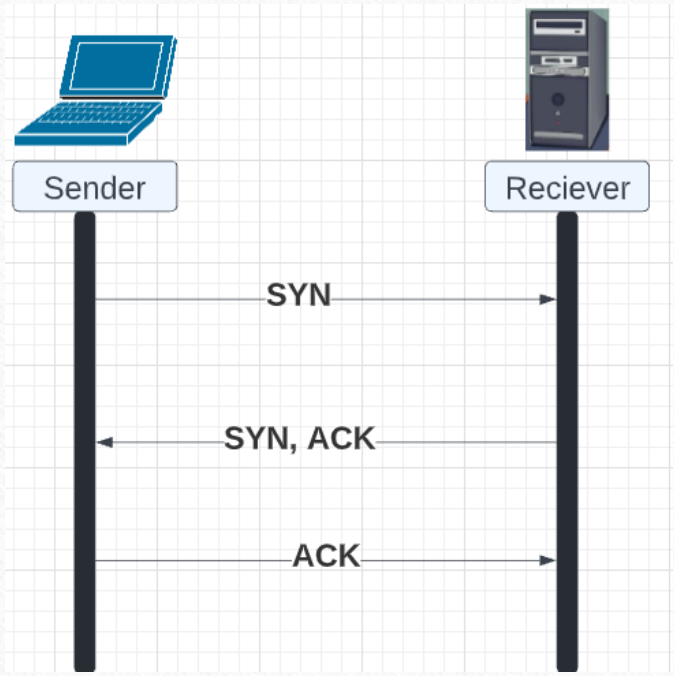
- Establish a UDP/TCP Protocol
- Compare the performance of block ciphers and stream ciphers over the established protocol using known ciphers such as AES and RC4
- Compare the Error tolerance for block cipher and stream cipher
- Compare the Performance based on Error tolerance
- Brief positive sides of the block cipher and stream ciphers

Classification of Cryptographic Algorithms

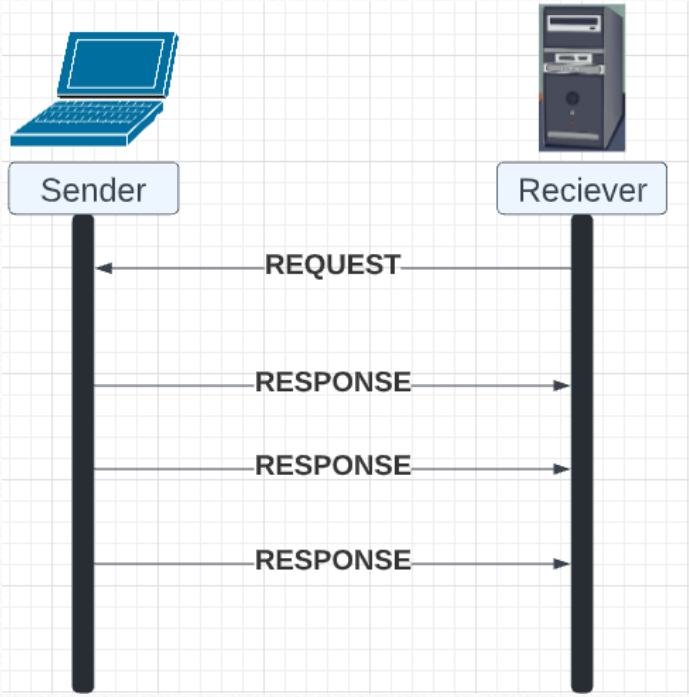


TCP vs UDP

TCP Schema



UDP Schema



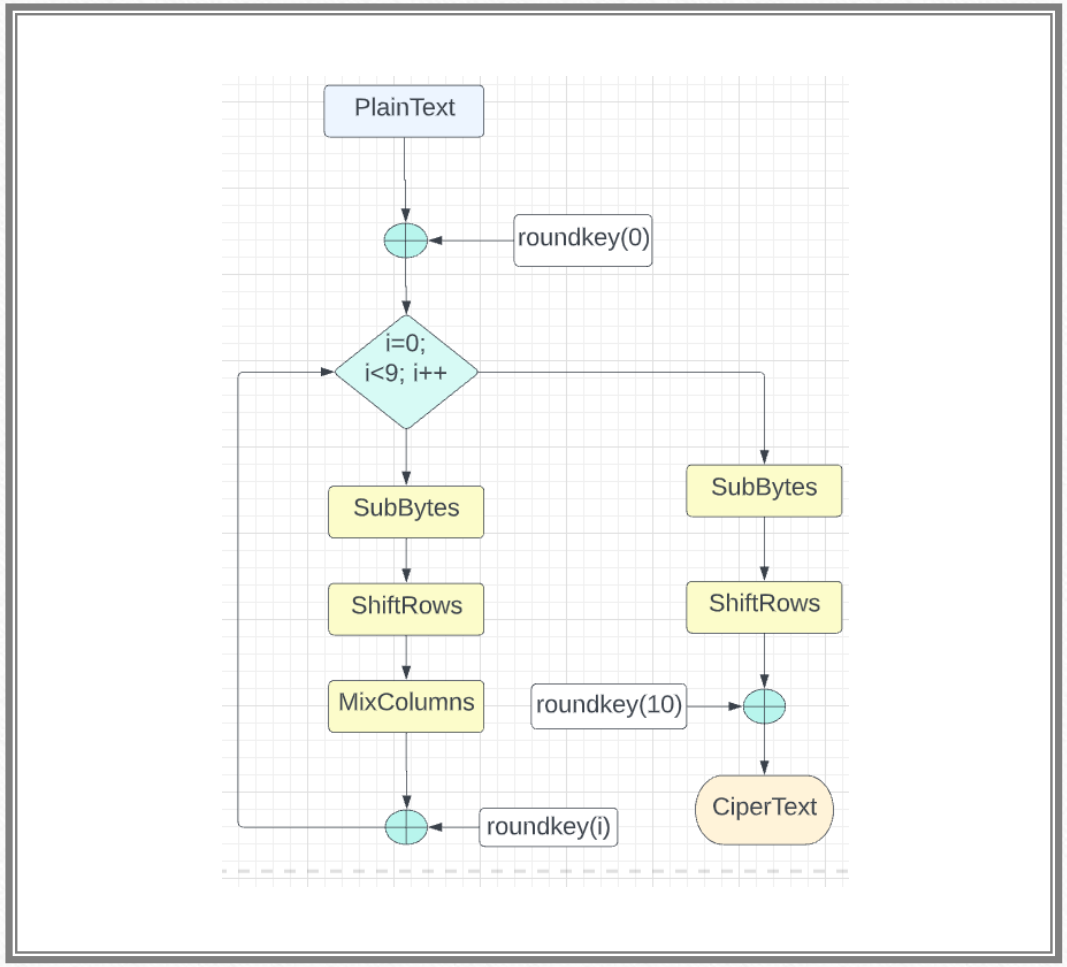
TCP vs UDP – Error Expectancy

- TCP retransmits lost data, hence error in TCP is almost zero
- UDP does not retransmit packets that is lost or corrupted
- UDP is more prone to errors than TCP

Block Cipher AES Algorithm

- Advanced Encryption Standard (AES)
- Unbreakable symmetric encryption
- Blocks are processed of fixed 128 bits size.
- Different bit sizes of key length results in 2^n number of keys as well as different number of Rounds.

Bit Width	Possible Number of Keys	Number of Rounds
128 bits	2^{128}	10
192 bits	2^{192}	12
256 bits	2^{256}	14

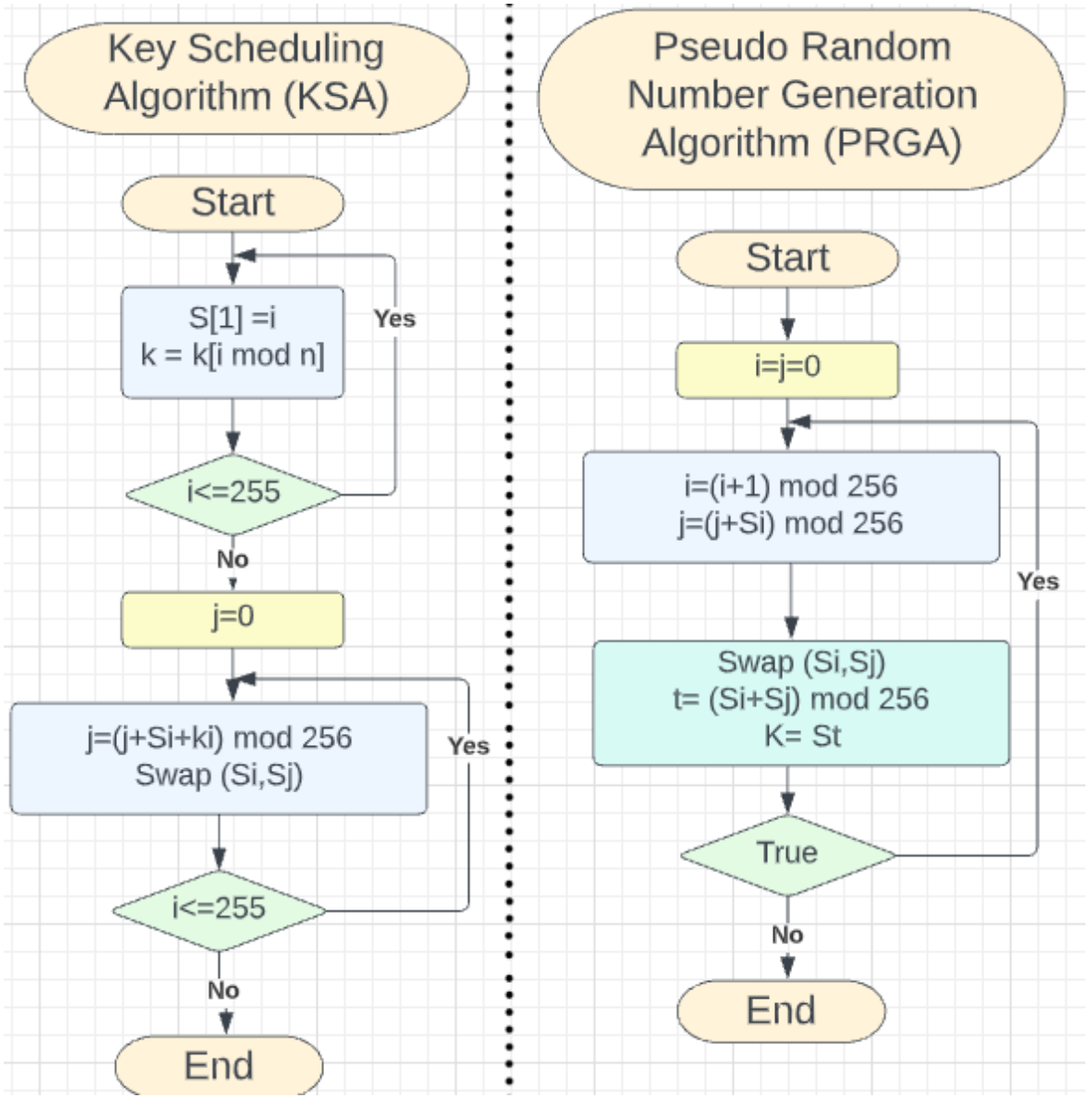


Block Cipher AES Algorithm

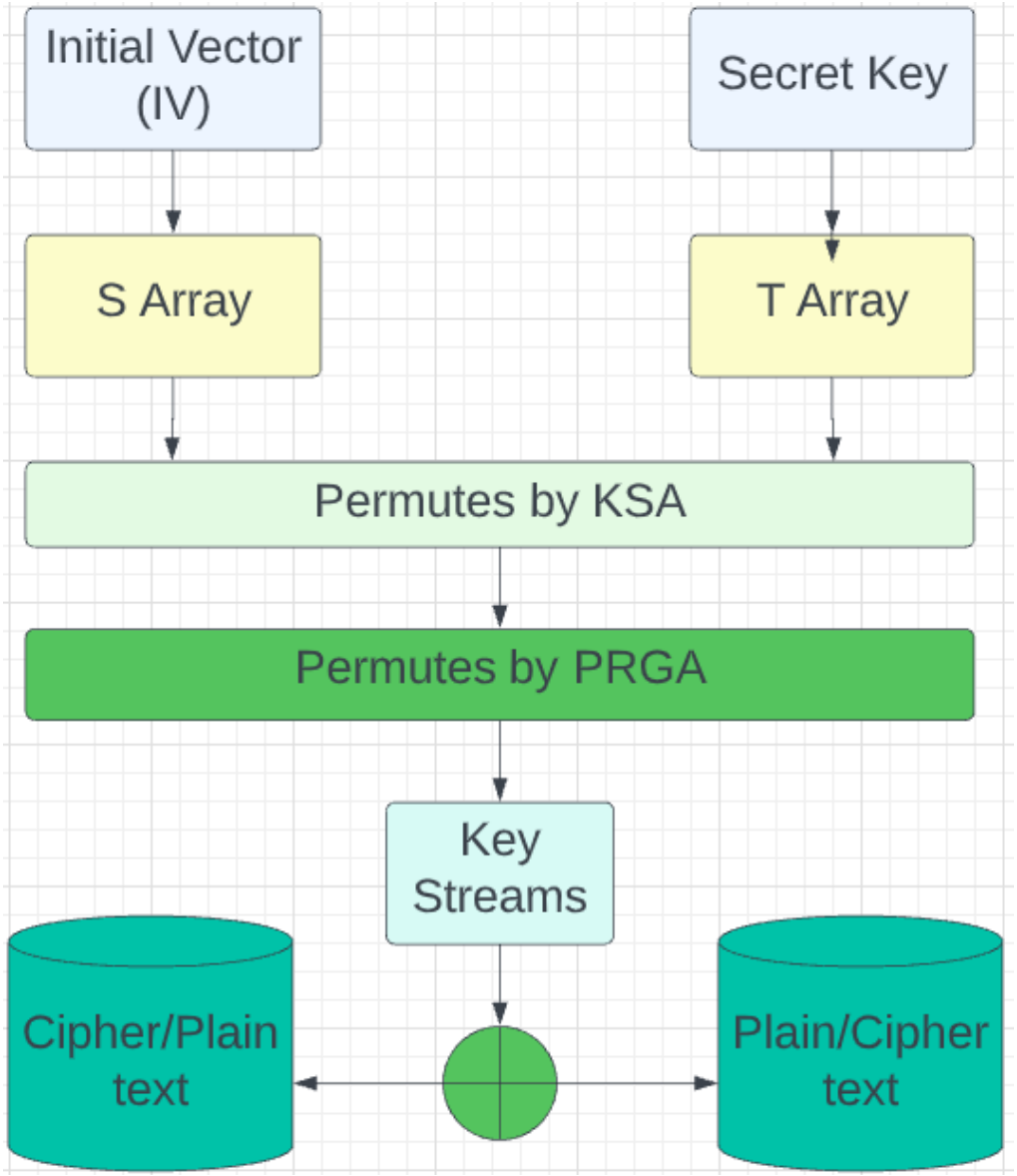
- Plaintext is processed in blocks
- First 9 rounds involve SubBytes, ShiftRows, MixColumns, Add round key
- Last round involves SubBytes, ShiftRows, Add Round key
- Ciphertext is achieved in blocks

Stream Cipher RC4

- One of the most widely used stream ciphers till today
- Key Scheduling Algorithm (KSA)
- Pseudo Random Number Generation Algorithm (PRGA)



Overview of RC4



Error Tolerance for the System AES vs RC4

- **TCP**
  - Block Cipher (AES) : Zero Probability of errors
  - Stream Cipher (RC4) : Zero Probability of errors
- **UDP**
  - Block Cipher (AES) : Error Tolerance is lower compared to RC4 (Blocks are affected)
  - Stream Cipher (RC4) : Error Tolerance is higher (errors are localized)

When to Use?

- **Block Cipher –** When Security matters, block ciphers are preferred
- **Stream Cipher -** Faster and Efficient (Devices with fewer resources)

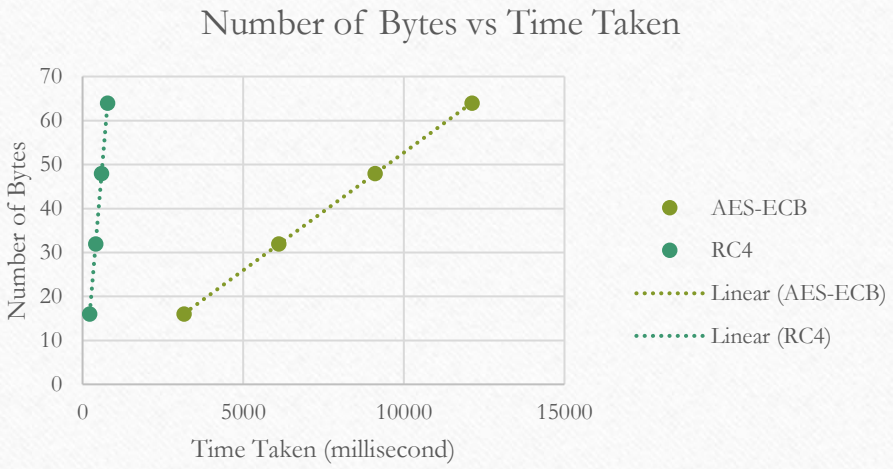
Results of Implementation

- **For TCP**

Stream cipher and Block cipher result in the same image that is a clear and precise image

Time Taken by Stream Cipher and Block Cipher Over TCP

- Block Ciphers (AES) take Comparatively more time (in milli Seconds) than Stream Ciphers (RC4) for the same number of bytes over the TCP Protocol



Stream Cipher	(USING RC4)		
No. of Bytes	EndTime	StartTime	TotalTime
16	1650987187876	1650987187654	222
32	1650987240351	1650987239946	405
48	1650987310314	1650987309726	588
64	1650987380255	1650987379476	779

Block Cipher	(USING AES-ECB)		
No. of Bytes	EndTime	StartTime	TotalTime
16 (1 block)	1650982079139	1650982075986	3153
32 (2 blocks)	1650982141342	1650982135236	6106
48 (3 blocks)	1650982205946	1650982196840	9106
64 (4 blocks)	1650982254744	1650982242621	12123

For UDP (Stream Cipher)

Threshold=0.01

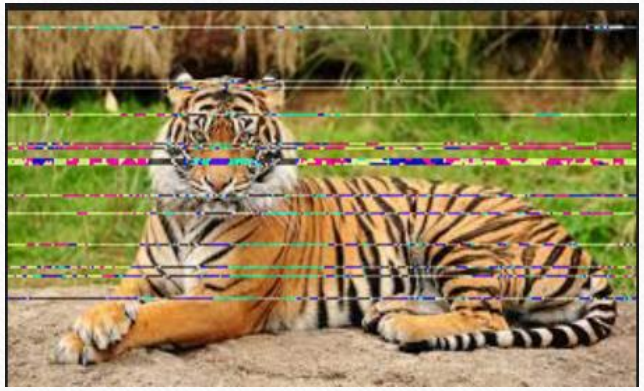
Threshold=0.1

Threshold=0.5

For UDP (Block Cipher)

Threshold=0.01

Threshold=0.1



Threshold=0.5


thank
you