

**Network Security**  
**CMPS-485**  
**Course Project-Phase 2**  
**Deadline: 9<sup>th</sup> April 2022**

**Project Title:** Performance comparison of state of art of block and stream ciphers over TCP/UDP protocol for different types of wired/wireless networks and applications.

**Student Name:** Talha Abdullah Punjabi (201903446)

## Abstract

The goal is of comparing the state of the art of block and stream cipher performance is to better understand how they are utilized to transmit data over the network and to investigate the various faults that cause differences in the transmitted data. Changes in message bits caused by the message being transmitted through wired or wireless media, as well as their impact on the original message, is to be analyzed. In terms of security based on continuous data encryption, stream ciphers have proven to be more efficient than block ciphers.

## I. INTRODUCTION

Cryptography has been used around the world since thousands of years with the goal to provide a safer transmitting of messages. The message sent is Plaintext and the confidential message is the ciphertext [1]. With the beginning of encryption in ancient times utilizing crude methods, to today's Quantum computer encryption techniques, encryption or secrecy were not a new phenomenon since the dawn of time [2]. An enciphering transformation takes place that converts the plaintext into the ciphertext. There are two ways in which the plaintext is processed that is block ciphers or stream ciphers. The input is processed one block of plaintext at a time with block cipher, whereas stream cipher processes input elements constantly and produces one output at a time [3][4]. These types of ciphers provide a real time operation, as

entire dataset is not delivered before decryption starts occurring [2].

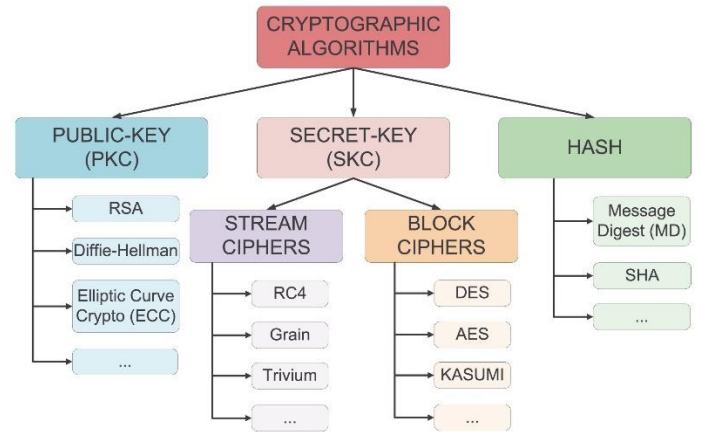


Figure 1 – Classification of Cryptographic Algorithms [5]

### I.1) Project Goal and Objectives

The project's goal is to compare and build mechanisms for different types of wired and wireless networks that use block cipher and stream cipher over TCP or UDP protocol. TCP is a more dependable approach than UDP since data is transferred from the sender to the destination without loss. Retransmissions in the TCP protocol offers to give the best performance takes more time than a UDP protocol. Errors in the output (i.e., image) will provide a quick indication of the performance of the block and stream ciphers over a specific protocol. The predicted outcome is for the stream to be far more bearable to errors than block ciphers. The project will also implement these mechanisms to show the error comparison over block cipher using AES with EBC and stream ciphers like RC4 to compare their performance on a UDP

protocol using Java / Python programming language.

## II. PROJECT DESCRIPTION

### A. Project Architecture – Individual Building blocks for the System

#### 1) Block Cipher- AES (ECB Mode)

The Advanced Encryption Standard (AES) is an unbreakable symmetric encryption that uses a single key for both encryption and decryption. Using the most advanced technologies, breaking into the weakest form of AES would take billions of years. [2]. AES uses block cipher processing of the plaintext. Usually, these blocks are of fixed 128 bits size. The key length of different bit sizes such as 128 bits, 192 bits, 256 bits results different number of keys.

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

Table 1 – Popular Bit Widths and their key size [2]

#### Steps used in AES [2]:

- 1) **Key Expansion** – key scheduling algorithm is used to generate keys

- 2) **Initial Round key addition** – Initial state of each byte is combined with block of round key.

#### 3) Round Step – (9, 11 or 13 times)

- i) **Sub Byte Step** – Substitution of bytes according to a table
- ii) **Shift Rows Step** – Last three rows are cyclically by 1, 2, or 3 steps

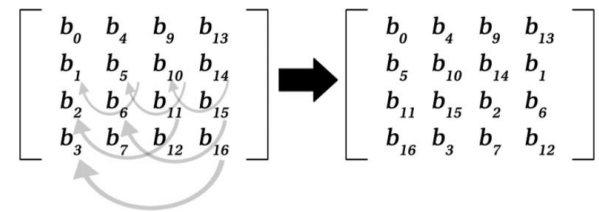


Figure 2- Shift Row Step [2]

- iii) **Mix Columns Step** – Combinations through multiplications of four bytes in every column
- iv) **Add Round Key Step**
- 4) **Last Round** – Takes place once and includes Sub Bytes, Shift Rows, and Add Round key.

These steps together lead to the formation of a ciphertext block that is AES encrypted.

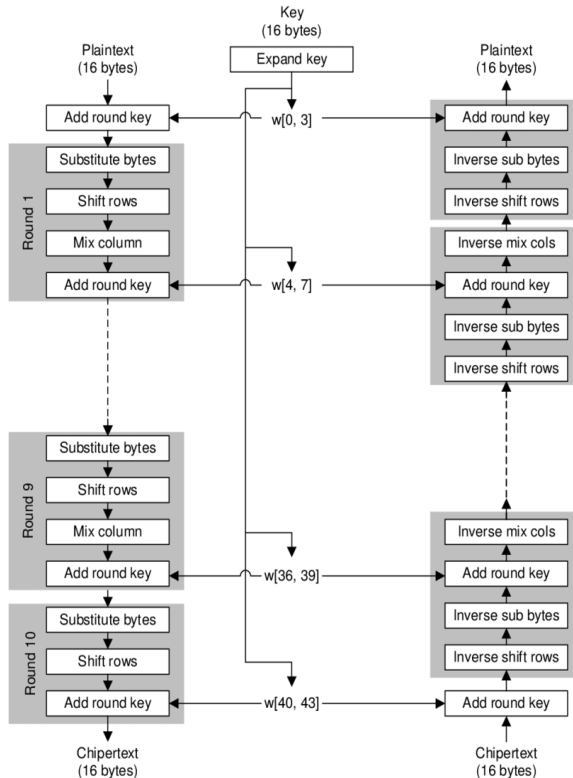


Figure 3 - Overview of AES Algorithm

## Electronic Cipher Book (ECB) Mode

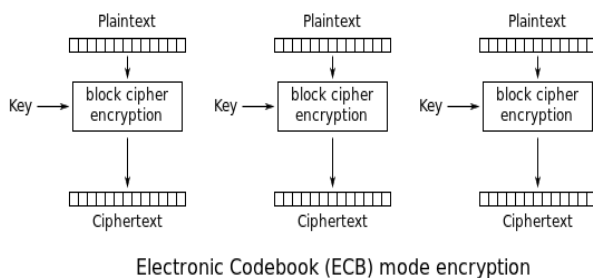


Figure 4- Block Cipher ECB Mode

Each block of plaintext is processed using an encryption with key to produce a ciphertext. An Error in a single plaintext will not affect other blocks as it is not a chaining mode.

## 2) Stream Cipher - RC4 Cipher

RC4 is one of the most widely used stream cipher which involves byte level manipulations; hence it is ideal for faster encryption.

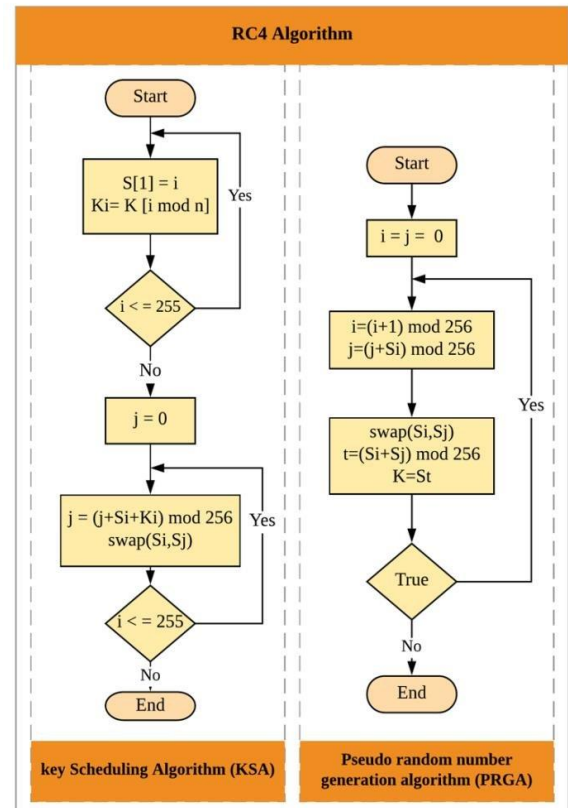


Figure 5-RC4 Stream Cipher [9]

Figure 4 shows the steps implemented by the RC4 Algorithm to produce the output of cipher stream. Stream ciphers deal with individual bits such as the case here in RC4 where individual bits are XORed and processed to give an output bitstream.

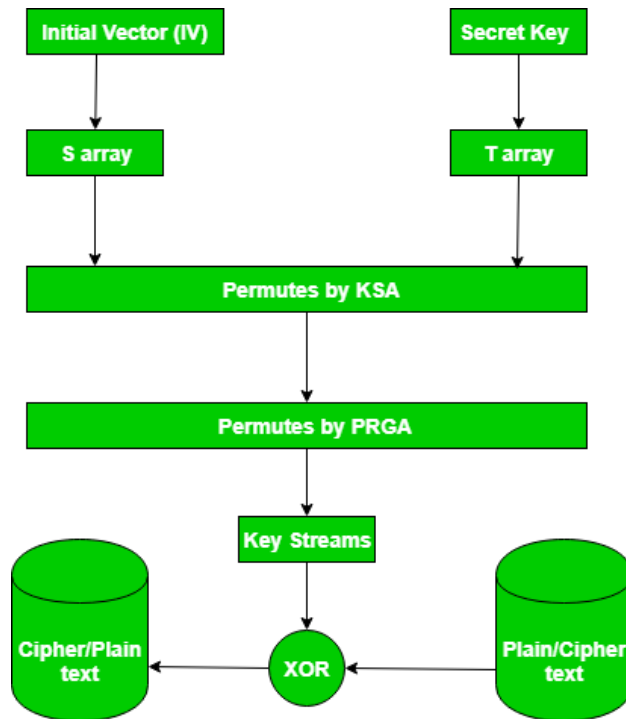


Figure 6 - Overview of RC4 Algorithm [9]

### 3) TCP Protocol

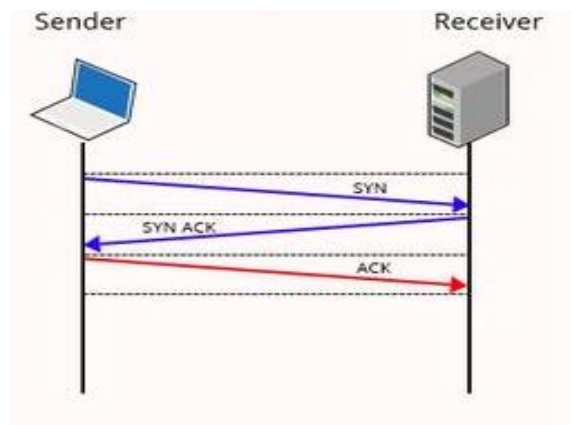


Figure 7- TCP Schema

TCP (Transmission Control Protocol) is a point-to-point connection-oriented transport protocol that sends data packets as an unstructured stream of bytes in an ordered sequence. TCP guarantees data reliability, end-to-end delivery,

resequencing, and retransmission until a timeout condition is met or data packets are acknowledged. Loss of packets triggers a retransmission process to retrieve the packet.

### 4) UDP Protocol

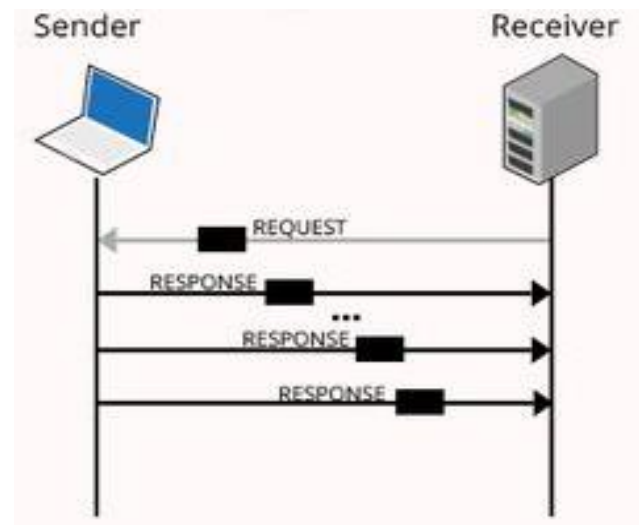


Figure 8- UDP Schema

UDP (User Datagram Protocol) is a connectionless transport layer communication protocol for establishing low tolerance and loss latency connections for the delivery of services or packets within or across networks. As an alternative to the TCP/IP protocol, it is combined with an internet protocol suite. Loss of packets do not force any retransmissions.

### 5) Error Expectancy: TCP vs UDP

As TCP is a reliable protocol, error expectancy is expected to be almost zero due to retransmission of lost or corrupted packets. While UDP is a connectionless protocol, it is not concerned about data loss. As a result, error expectancy for the UDP protocol might vary from packet to packet

and is obtained to be higher than the TCP protocol.

## 6) Error Probability for the System

TCP has a zero-percentage error probability when used with any encryption. The error probability for UDP varies depending on the block or stream ciphers used. In the case of stream ciphers, individual bits are affected, whereas any faults during data transfer across the network affect the entire block for the case of block cipher. Affected individual bits may cause slight or unnoticeable errors in the outputted image compared to the block cipher where the loss or unordering of a packet can cause a noticeable error to the outputted image.

Therefore, in UDP,

**Performance (Stream Cipher) >**

**Performance (Block Cipher)**

as

**Error tolerance (Stream Cipher) >**

**Error tolerance (Block Cipher)**

## 7) Performance comparison of Block cipher vs Stream cipher on TCP and UDP

TCP is a reliable protocol. Hence, there is no loss of packets during the transmission. If such a case happens, TCP will try to retransmit the packet. Hence, there won't be a difference in the output for block cipher or stream cipher. While in the case of UDP, there is no retransmission and some packets being lost is of no concern to UDP. TCP takes more time as compared to UDP to retransmit some lost packets even then this

maybe of small difference. Even though the image or information is delivered perfectly by TCP, it still takes additional time to deliver the packets as compared to UDP. Block cipher can lose blocks and hence greater error in the outputted image. While stream ciphers are more resistant due to loss of few bits here and there. Thus, stream ciphers have better performance although block ciphers are more secure.

## 8) Performance Graph: Block cipher vs Stream Cipher algorithms

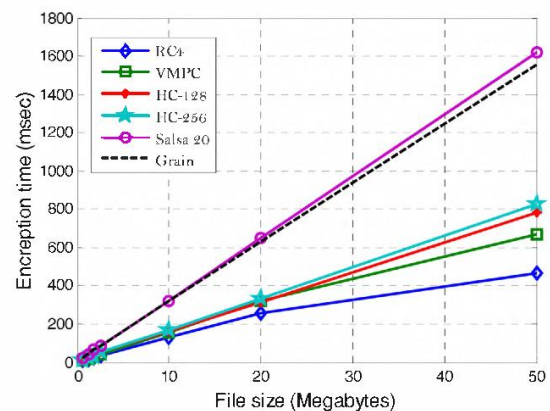


Figure 9- Performance of Stream Cipher Algorithms [8]

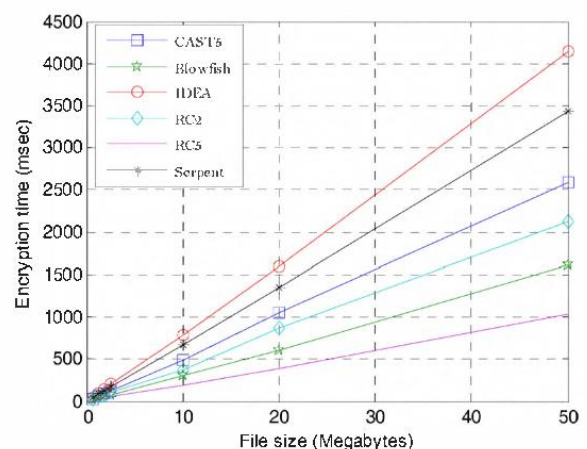


Figure 10- Performance of Block Cipher Algorithms [8]

## Elementary Results [Code Attached]:

### USING PYTHON

#### i. Using TCP Protocol with stream cipher (Code Attached)

Sent Image:



Received Image:

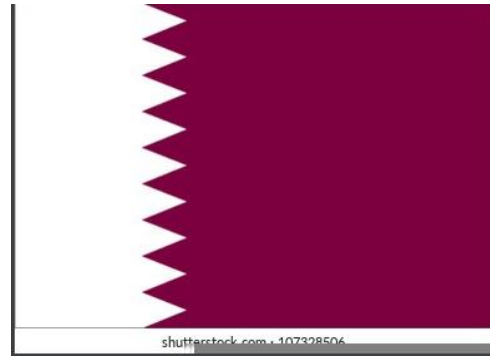


#### ii. UDP using Stream Cipher [Code Attached]

Sent Image:



Received Image:



### USING JAVA

Using UDP protocol without any Error Percentage

[Code Attached]

Sent Image:



Received Image:





## Conclusion:

To summarize, each cryptographic algorithm provides security in some way. The algorithm to be utilized is determined by the application's requirements. The results will reveal that RC4 is unquestionably more effective than AES in terms of performance and error bit localization. It is also worth noting that AES is more secure than RC4, thus can be fulfil security requirements of some applications.

As observed, UDP with stream ciphers produces very less error, hence, does not affect the overall view of image.

While TCP with stream cipher produces a replica of the received image since there is no loss of packets.

Using java, we checked the transmission of UDP protocol without any error percentages [Hence acting as a TCP Protocol]. Thus, we obtain a clear image from the transmitter to the receiver.

## Future Work:

Sending an image using AES (Block Cipher-ECB) on UDP [Java Implementation]

Sending an image using a stream cipher algorithm- RC4 on UDP [Implementation]

## References

- 1) Al-Saady , .. . (2013). A Little Cryptography through Number Theory = التشفير عبر نظرية الأعداد. Thesis (Master)--Taibah University, 2013.
- 2) Robert Ciesla,. (2020, August), *Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography* (2020)
- 3) Wikipedia contributors. (2022, January 28). Block cipher mode of operation. In *Wikipedia, The Free Encyclopedia*. Retrieved 16:39, March 23, 2022, from [https://en.wikipedia.org/w/index.php?title=Block\\_cipher\\_mode\\_of\\_operation&oldid=1068383852](https://en.wikipedia.org/w/index.php?title=Block_cipher_mode_of_operation&oldid=1068383852)
- 4) Wikipedia contributors. (2021, October 26). Stream cipher. In *Wikipedia, The Free Encyclopedia*. Retrieved 16:40, March 23, 2022, from [https://en.wikipedia.org/w/index.php?title=Stream\\_cipher&oldid=1051986324](https://en.wikipedia.org/w/index.php?title=Stream_cipher&oldid=1051986324)
- 5) Antonio J. Acosta, Tommaso Addabbo, Erica Tena-Sánchez, (2016, December 13),. *Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview.* (2016)



- 6) TCP/IP vs UDP: What's the Difference. December 17, 2018. By *Nisha Jiju* (2018)
- 7) Sharif, S.O., & Mansoor, S. (2010). Performance analysis of stream and block cipher algorithms. *2010 3<sup>rd</sup> International Conference on Advanced Computer Theory and Engineering (ICACTE), 1*, V1-522-V1-525.
- 8) Mini Rani Sharma, Vikash Kumar Agarwal, Nitish Kumar, Santosh Kumar, *Integrated Intrusion Detection System (IDS) for Security Enhancement in Wireless Sensor Networks, Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks*, 10.4018/978-1-7998-5068-7.ch009, (177-196), (2020).
- 9) *ARSMS: A Hybrid Secured SMS Protocol for Smart Home using AES and RC4* - Scientific Figure on ResearchGate. Available from: [https://www.researchgate.net/figure/Flowchart-of-RC4-Algorithm\\_fig1\\_323783954](https://www.researchgate.net/figure/Flowchart-of-RC4-Algorithm_fig1_323783954)