Introduction

Motivation and citation

Defining the algo

What point completed

Future work

Bibliography

Project Report

On

**Implementing a simple encryption and decryption algorithm based on some basic ciphers.**



Department of Computer Science and Engineering

Tezpur University

B. Tech Project

4th Semester

Under the Guidance of

**Dr. Arindam Karmakar**

Professor

Department of CSE

Tezpur University

**Submitted By**

**Dhiraj Saharia(CSB17026)**

**Ravi Roushan Kumar(CSB17078)**

(B. Tech, Computer Science & Engineering, Tezpur University)

**Acknowledgement**

This project ― Implementing a simple encryption and decryption algorithm using some basic ciphers was a great learning experience for us and we are submitting this project work to **Department of CSE, Tezpur University.**

The satiation and euphoria that accompany the successful completion of the project would be incomplete without mentioning name of the people who made it possible. It is my pleasure to express our sincere thanks to all of them.

First and foremost, we would like to take this opportunity to thank and express our deep sense of gratitude to our Professor Dr. Arindam Karmakar(Professor of CSE Department)**.** We are greatly indebted to him for providing his valuable guidance at all stages of the study, his advice, constructive suggestions, positive and supportive attitude and continuous encouragement without which it would never have been possible to complete the project.

We are very glad to mention the name of Bidon Saha(CSB17008) for his help and interest towards our project.

**Sincerely**

**Dhiraj Saharia(CSB17026)**

**Ravi Roushan Kumar(CSB17078)**

**Introduction**

Network security is concerned with the protection of network resources against alteration, destruction and unauthorized use, cryptography and encryption are most critical components of network security.

Networks take all kind of sensitive data and security play a vital role of any wireless network system. Security certify level of data integrity and data confidentiality as maintain wired network, without accurately implement security measures and wireless network adapter come within range of the network adapter. Security is high lack, laziness, and lack of knowledge and employee are not aware of these things, especially in small organisation and home, every organisation need to aware and training for employees’ time to time.

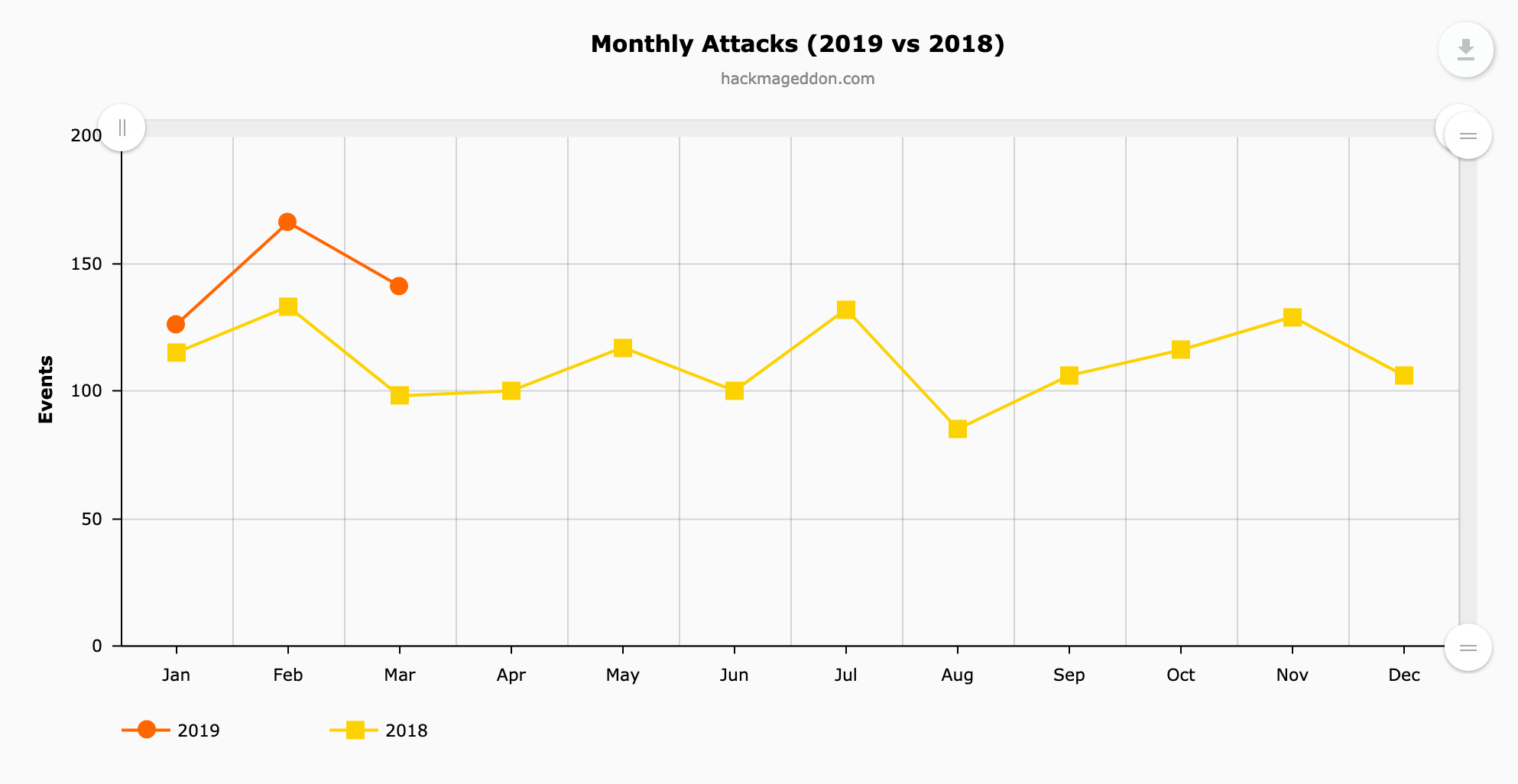
Role of Cryptography –

Nowadays business operation decentralization and correspondence growth of computer network is the number one driver of concern about the network security. As far as security concern, many organisation networks are accidently waiting to occur, such accident will occur is impossible to predict but security breaches will occur. The following five basic uses of cryptography in network security solution are:

Confidentiality – Cryptography gives confidentiality through changing or hiding a message and protects confidential data from unauthorized access and use cryptographic key techniques to critically protect data;

Access control – Only authorized users (login & password) can access to protect confidential data etc. Access would be possible for those individual that had access to the correct cryptographic keys; (Mitchell, M, 1995)

Integrity – Cryptographic tools give integrity verify that permit a recipient to authenticate that message transformed and cannot prevent a message from being transformed but effective to identify Either planned and unplanned change of the message

 Fig. – Monthly Cyber-attacks from 2018-19

As the graph clearly shows that the number of cyber-attacks is increasing safety measures are a must for any big corporation to protect its users from any kind of data breaches or identity theft.

Some cyber security statistics –

* 90% of remote code execution attacks are associated with crypto mining.
* 92% of malware is delivered by email.
* 56% of IT decision makers say targeted phishing attacks are their top security threat.
* 77% of compromised attacks in 2017 were file less.
* The average ransomware attack costs a company $5 million.
* It takes organizations an average of 191 days to identify data breaches.
* 69% of companies see compliance mandates driving spending.
* 88% companies spent more than $1 million on preparing for the GDPR.
* 25% of organizations have a standalone security department.
* 54% of companies experienced an industrial control system security incident
* 61% of organizations have experienced an IoT security incident

**Motivation and Citation**

Due to the following points we tried to create our own algorithm that was easy to understand, implement and test.

* Cybercrime is increasing day by day with the advent of new technologies.
* Most cryptographic algorithms are highly mathematical and require formal methods to prove its effectiveness.
* Some algorithms are very difficult to compute by hand due to the use of very large numbers used.
* Most algorithms are tested on an abstract machine first, due to this fact the corresponding machine architecture becomes complicated sometimes.
* Cyber security is one of the most demanded skills in the industry now with huge potential.
* To protect the data of users

**Citation –**

Resources taken from Internet –

Links –

[1] - <https://en.wikipedia.org/wiki/Caesar_cipher>

[2] - <http://practicalcryptography.com/ciphers/caesar-cipher/>

[3] - <https://www.geeksforgeeks.org/xor-cipher/>

[4] - <https://en.wikipedia.org/wiki/XOR_cipher>

[5] - <https://crypto.stackexchange.com/questions/19470/how-is-xor-used-for-encryption>

[6] - <https://en.wikipedia.org/wiki/Ones%27_complement>

**The Algorithm**

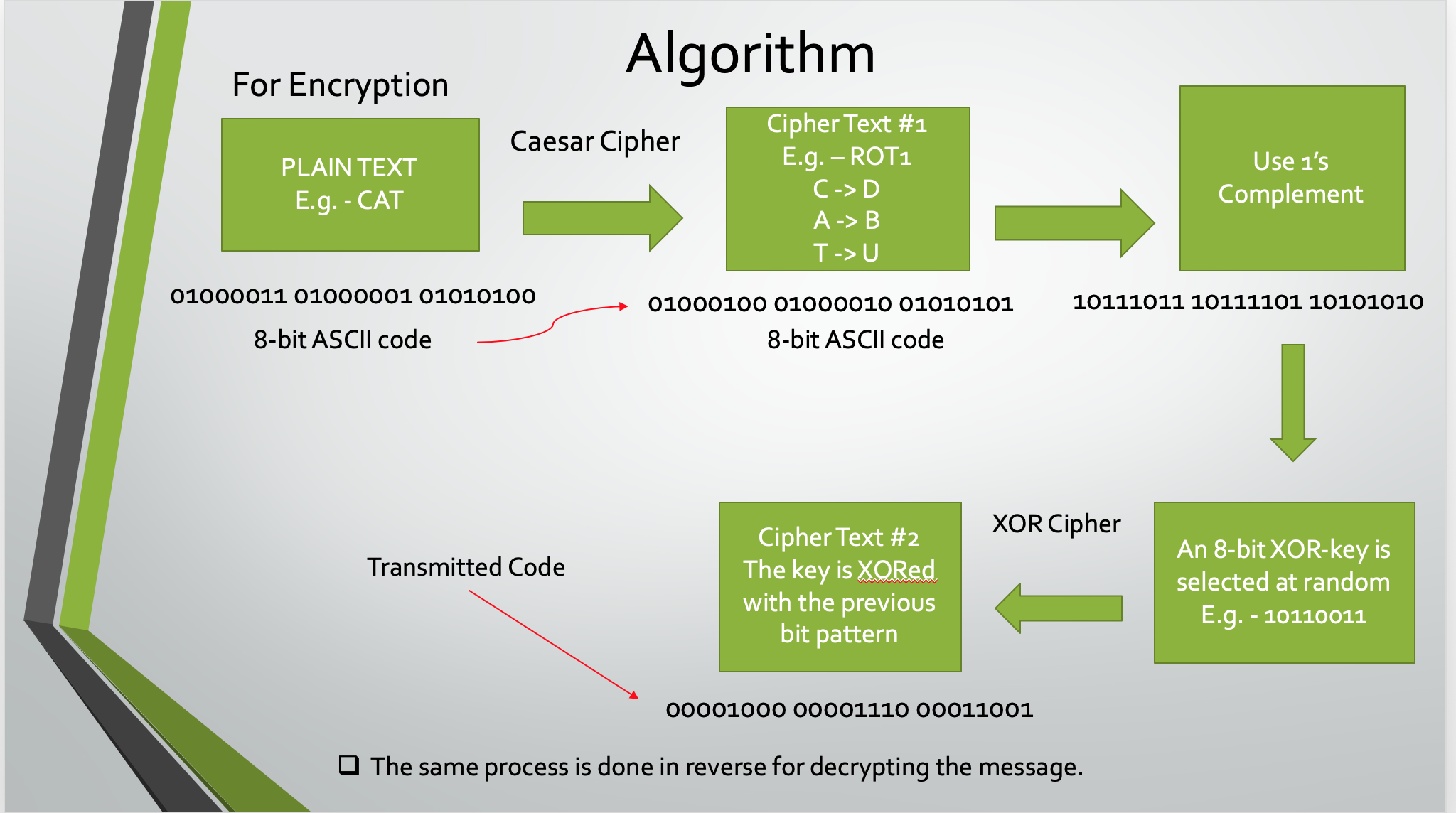
Steps for the algorithm –

* First the algorithm takes the plain text message as the input.
* It is then converted to the cipher text through a series of steps.

1. First every character is shifted by the rotation value specified by the sender in the Caesar cipher and converted to its ASCII code.
2. Then the ASCII code is converted to the corresponding 8-bit binary representation.
3. Then the one’s complement of the binary code is taken.
4. The whole bit string is now XOR-ed with a specific 8-bit XOR key specified by the sender which is to be remembered for the whole process.
5. The resultant bit string is now the encrypted data which can be now transmitted safely.

* The whole process is repeated in reverse for decryption process (converting cipher text to plain text message). Only the XOR key and the Rotation value is to be specified.

For e.g.



**Future Work**

* Implementing this algorithm using a raspberry pi to send the encrypted data in a network. Since the algorithm is simple it does not require much hardware resources and can be implemented in limited hardware also.
* We can create a simple messaging app using this algorithm to keep the messages safe. This app could have three functions –

to encrypt an outgoing message string, to decrypt an incoming string and to send the data through it.

* We can improve this algorithm by using some error correcting code like Hamming code. When the data bits would be travelling inside the network it might encounter noise and other impairments, therefore we could use error detecting and error correcting as well as only error detecting codes also.
* We can strengthen the encrypted data by using different 8-bit XOR key for every character along with different rotation values with a particular periodicity. To increase the randomness in the encryption process and make it less vulnerable to simple cryptanalysis techniques.