Proceedings of the International Conference on Communication and Electronics Systems (ICCES 2018)
DVD Part Number:CFP18AWO-DVD; ISBN:978-1-5386-4764-6

Information Technology Language Encryption Register(ITLER)

S. P. Maniraj [1], S. Shriram [2], Meghna Anand [3], P. Sai Prasanth [4], Anurag Chakraborty [5]

Assistant Professor(Sr.G) [1], [2,3,4] UG Scholers

SRM Institute of Science and Technology, Chennai

maniraj.p@rmp.srmuniv.ac.in [1],

shriram@ankor.us [2], meghna@ankor.us [3], saiprasanth1303@gmail.com [4], anurchak@gmail.com [5]

***Abstract*— In this paper we've proposed a hand-held device that can be connected to your phones that allows the encryption and decryption of text messages. The device that inspired us is called an Enigma machine, which is a polyalphabetic cipher. The Enigma machine is taken as the base of what our model envisions. The deciphering of this encryption system cannot be done that easily even by frequency analysis and other cryptanalysis techniques. These enigma machines were used in the Second World War to send and receive encrypted messages, but those machines were far too bulky and were in the form of a typewriter. We have come up with a much more efficient and simpler way to send encrypted messages in a much smaller scaled device, a TFT screen (3 inches approx.).In simpler terms, the device connects to your smartphone to send and receive encrypted messages, pushing the boundaries of the Enigma machine right into the 21sh century.**

Keywords—Enigma cipher, smartphone, Bluetooth, encrypted messages

I. INTRODUCTION

We propose a continuous encryption framework that chips away at best of a present informing stage in light of Enigma. The inexact nonlinear instrument and the polyalphabetic figure of the encryption framework settles on it a decent decision for a continuous message encryption. The present situation enables clients to send and get messages. Yet, these are by and large always observed by remote insight and other identification frameworks that logs and stores the client information. Indeed, even huge corporates like Facebook confront information breaks and spilling of client information to people or organizations that prompts malignant movement. Our continuous model works in parallel with an informing framework and scrambles and decodes on the fly. The gadget is associated with the phone utilizing Bluetooth and once the association is set up the gadget goes about as a virtual console and works the same way as a normal keyboard would. With a convenient and a more secure encryption framework, we hope to accomplish a more secure method for communication between the people today. The present model of encryption present doesn't solve the issue of message being read by offhand parties. This is due to the fact that most messaging services use something called as end to end encryption. Though this type of encryption does solve the issue of messages being 'caught' between phones, it still doesn't solve the problem of people reading these messages on the user end device. This has led to data loss and confidential information leakage. To counter this issue or to say tackle this issue, we have developed a hand-held device that lets a user encrypt a message on the fly and send the encrypted information to another device. The recipient of the message can then read the encrypted message by using the same hand-held device that was used for encrypting the message. By implementing this technique, we have what we believe solved the issue of data loss since this method adds another layer of security for any messages sent using the current messaging platforms.

II. RELATED WORK

Zhi-liang ZHU, Chao BU, Hui LI and Hai YU's paper, A NewChaotic Encryption Scheme Based on Enigma Machine [1] presents to us the idea and pretense of history's most famous encryption device- The Enigma device. The encryption process of the enigma device is explained as a process that involves many mechanical moving parts that constitute to a very fool proof method of encryption. The design of the device as explained by the authors is quite simple. But this simple device can generate up to 15^{24} combinations. This particular paper is presented by the authors who explain the chaos theory of encryption. This chaos theory takes advantage of the enigma's non-linear mechanism with the chaos controlling the encryption process. They have observed that by using this new chaos theory of encryption, the randomness of plain text has increased and also, they have seen improvement in the security of the encryption scheme. They have also observed that the results of encrypting images and letters proved that this novel encryption scheme shows good performances in the analysis of key sensitivity related coefficient between adjacent pixels and differential cryptoanalysis.

Implementation of Hummingbird 1sCryptographic Algorithm for Low Cost RFIDTags using LabVIEW [2] by P.V.G. Raj Pritha and N.Suresh is a paper which explains the encryption of data by using a low-cost effective encryption like the Hummingbird encryptions for RFID applications. The Hummingbird is a novel ultra-light weight cryptographic encryption used in this paper in mutual authentication protocols. This Hummingbird algorithm has a precise response time and the design of the small block sizes present will reduce the overall power consumption requirements. This is due to the fact that the Hummingbird encryption consists of both block and steam ciphers. In this paper the authors have used the RFID tags as both reader and encryptor. This algorithm is performed using the LABVIEW software. The authentication protocol for the Hummingbird algorithm is of 3 phases. The first phase is the authentication phase where the reader will determine if the correct key is shared with a particular card. The second phase is the mutual

authentication of a reader and a tag. The final phase is where the command authenticated by the reader is received and executed by the encryption RFID tags.

Implementation of Enigma Machine Using Verilog on an FPGA [3] by Deniz Engin, Berna Ors is a paper that instantiates on using the Enigma machine with a Field programmable gate array and Verilog hardware description language. The authors explain the nature of the Enigma machine as a poly alphabetic cipher. In other words, even if the input given is a repeated letter, the output can be a different letter. This constitutes the fool proof history of the Enigma machine cipher. The authors use a 20th century Enigma machine (The ones that were used during World War 2) and fitted them with a FPGA (Field Programmable Gate Array) and HDL protocol. To make this arrangement work, they also added a few additional keys and plugboard settings. Then 5 major tests were performed under controlled conditions to verify the credibility of using HDL and FPGA in a Enigma machine. The first test being the plugboard test was performed and the expected results were obtained. The reflector test also portrayed similar outputs with modifies system working without any error. The rotate test is performed by rotating the wheel, reading the input of the machine and checking if the corresponding outcome was obtained using the FPGA and HDL protocol. The rest two tests, namely the wheel test and the enigma test all resulted in expected outputs with little to almost no deviation. All the tests were conducted using the ISIM simulator and spartan 3E. The results concluded that a modified Enigma machine with FPGA and HDL protocol is possible.

The Research of Information Hiding and Extraction Based on QR Code PositioningFunction [4] by MumingLi, Peng Cao, Lifang Yu, Liuping Feng, Jianbo Chen and Jing Wang is a paper which describes a process by which real time positioning of QR code scanners can lead to the hiding and extraction of data. The authors explain that this can be done by using a printing method called Digital halftone printing which converts a continuous grey image into a binary image and uses the density of dots that include black and white to represent the grey value of the greyscale image. So when a phone reads the information of a printed image, it can utilize the positioning function of QR two dimensional code to accurately correct the image. The function formula of square dots and diamond dots that the authors use in this paper are as follows:f(x,y) = l-(|x| +|y|) and f(x,y)=l-(lxl+ |y/0.75|). After implementing this Digital halftone printing and the square and diamond dot algorithm, the authors observed a stable result that shows that this method effectively solves the technical bottleneck problem that mobile phones face when reading the hidden information in the microstructure of a printed image.

III. MODEL

We have proposed a system through which one can send and receive encrypted data through current messaging platforms. The advantage of this system is that it was designed with the current security exploits in mind. It is not susceptible to any means of skimming, phishing, package switching and keyloggers. This is due to the fact that in our model, the data is encrypted before it is sent. While current security techniques are all based on encrypted the data after it has been sent or securing the transmission process. This results in a more secure and resource saving system. The

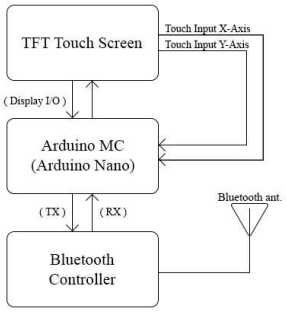

Fig 1: The primary System

System consists of an external encrypting device that connects to a mobile or any electronic message sending device like pagers and beepers. The device itself consists of an ardruino Nano board coupled with a TFT screen. The Nano board acts as the bridge between the peripherals and the code. An additional Bluetooth keyboard can be connected to the arduino board which makes it easier for the user to type and send messages. So, the arduino board along with the Bluetooth module and the TFT screen constitute the primary system [Fig 1].

The device can also rely on the existing software keyboard on every phone. The connection between the phone and the module is made with the help of the Bluetooth module. But since some phones may already be tampered, the risk of a keylogger present is high. So we have designed a secure android keyboard app that can connect to the Bluetooth module with ease. Since the Bluetooth module is a Bluetooth 4.1 device. The connection between the app and the board exhibits no stutters or jitters. The Bluetooth device along with the phone app and the Bluetooth monitor constitutes the Bluetooth module of the device [Fig 2]. The device is split into various modules so that no module may interfere with another and cause the device to stop functioning. All these modules work together to function as a single unit. The flow of the system is shown in Fig. 3

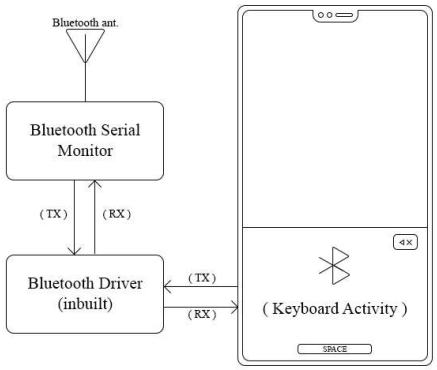

Fig .2: The Bluetooth module

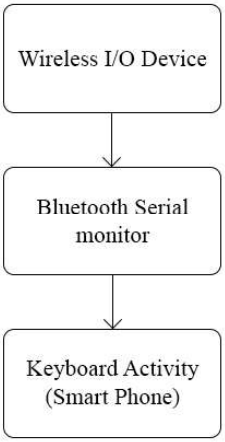

Fig. 3: The Flow of the System

.

IV. Future Work

In our iteration of the Enigma machine, we have implemented a method of encryption with which users can send messages without fearing if anyone will be able to snoop ton their messages. But this instance of the model will not be the final produced model. We plan to decrease the size of the components so that the device can be carried anywhere. We are also trying to increase the battery capacity of the device since active Bluetooth drains a lot of power for a device this small and the device has to last for a whole day. Though increasing the battery capacity of the device may lead to an increase in the overall size of the device. But keeping this in mind, we plan to decrease the overall size as much as possible. We also plan to reduce the overall production cost of the device and also make it more appeasing to the casual user.

V. CONCLUSION

This paper showcases the handheld encryption device which was modeled after the Enigma machine used in the Second World War. This device provides the user with the ability to send messages to another device without the fear of online snooping. The device can be connected to the convenient Bluetooth keyboard which allows the user to send text which is first encrypted before sending it to the receiver. The receiving end also has a similar device which decrypts the message before displaying it to the user. The message can only be decrypted with the help of the decrypting device. This eliminates the issue of people reading your messages on a phone. The device was tested using the existing WhatsApp messaging platform and was results obtained concluded that the device is functioning properly.

VI. REFERENCES

[1] A New Chaotic Encryption Scheme Based on Enigma Machine, Zhi-liang ZHU, Chao BU, Hui LI, Hai YU,IEEE, 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications, pg 198.

[2] Implementation of Hummingbird 1sCryptographic Algorithm for Low Cost RFIDTags using LabVIEW, P.V.G. Raj Pritha and N.Suresh, ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India, ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE.

[3] Implementation of Enigma Machine Using Verilog on an FPGA, Deniz Engin, Berna Ors, IEEE.

[4] The Research of Information Hiding and Extraction Based on QR Code PositioningFunction, MumingLi, Peng Cao, Lifang Yu, Liuping Feng, Jianbo Chen and Jing Wang, 2016 2nd IEEE International Conference on Computer and Communications, pg 589.

[5] Rebuilding the bombe, IEE REVIEW NOVEMBER 2001, pg 7-10.

[6] Alan Turing andBletchley Park, Charles SeveranceUniversity of Michigan, Published by the IEEE Computer Society, 0018-9162/12/$31.00 © 2012 IEEE.

[7] A simple EnigmaA kit Replicatesthe infamousciphermachine, resources_HANDS ON, SPECTRUM.IEEE.ORG, north american, JAN 2015, pg 19-20.

[8] https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

[9] http://www.cryptomuseum.com/crypto/enigma/hist.htm

[10] http://practicalcryptography.com/ciphers/enigma-cipher/