www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7685-7689

Caesar Cipher Cryptographic Method Along With Bit-Manipulation to a Message to be encrypted and digest for RFID credit card security

Rohit Sharma, Dr. P.K. Singh
Research scholar
Teerthanker mahaveer university
Moradabad

Professor
IIMT Engineering College
Meerut
Email- rohit_techelectro@yahoo.com

Abstract: A lot of sophisticated problems we have to face during the security of RFID credit card. In this paper, author using a new approach to make RFID credit card more secure. The main objective of this paper is to provide a method along with encryption and digestion of incoming and outgoing data to RFID credit card. In this paper we presents a new cryptographic approach to exclude the repetitive terms in a message, when it is encrypted and digest [1], so that it is not easy for any adversary to retrieve or predict the original message from the encrypted message. . By using cryptographic approach, we can improve the security by encrypting the plain text data to cipher text data. If we individually using Caesar cipher substitution and cryptographic hash function, then obtained cipher text is easy to crack. I proposed a perspective approach on combination of techniques substitution and digestion. We can eliminate the fundament weakness by combining Caesar cipher with cryptographic hash function technique.

Keywords: RFID Credit card, Encryption, Digestion, Caesar cipher, cryptographic hash function

I. Introduction

RFID credit cards are very popular because it has the contactless payment transactions facility. That why it is very fast, easy, more reliable magstripe transactions, and it need only physical proximity between the credit card and the reader. But these features are not so beneficial if we talking about security and privacy vulnerabilities. Traditional credit cards need that a physical contact to obtain information like cardholder's name and the credit card number from the card. RFID credit cards not needing any physical contact, it can transmit and receive the sensitive data using a small radio transponder that is activated by a reader. In the remainder of this paper we will examine, how much the RFID credit card is secured, and what algorithm we have to apply to make it more secured [2].

I.i- Playbook for a crook in RFID credit card

1. The Setup

Thief connects a card reader to a net book in briefcase, which hide the devices.

2. The swipe

Adversary carries briefcase very close to consumer's pocket, for reading the contactless cards.

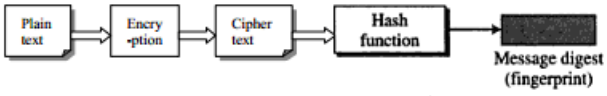
3. The display

Then Card information obtained by adversory is displayed on a computer attached to a magstripe-writing device.

4. The clone

By Brown Bird Design, we can make a counterfeit card by using blank magstripe card.
An attacker can simulate many transactions as desired after spending an hour with a transaction-counter card. With the legitimate card a counter-synchronization is present that faces by the attacker, but this problem does not a level of difficulty.

It will be interesting to see, as time goes on, and technology gets smaller and cheaper, if any major fraud issues are reported with the technology. While there are some benefits to the RFID-enabled credit card transaction concept, for the customers, the merchants, and the card issuers, the numerous security flaws and attacks seem to beg the question of how secure the concept really is [1]. To overcome all these problems, we introduced a Cryptographic Method Along With Bit-Manipulation to a Message to be encrypted and digest for RFID credit card security [3].



Proposed Model

Caesar Cipher Cryptographic Method is used for encryption. To preserve the integrity of a message, the message is passed through an algorithm called a cryptographic hash function. The function creates a compressed image of the message.

II. Encryption

Caesar ciphers also named as the shift cipher. Caesar's code or Caesar shift is a very simple and mostly known encryption technique. In this substitution cipher each plaintext letter is replaced by a letter some fixed number of positions down the alphabet. For example, when we have a left shift of 3, D would be replaced by A; E would become B, and so on. This method is known as Julius Caesar [4].

We can also represent the encryption by using some modular arithmetic by transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25, for a letter x by a shift n, Encryption can be write mathematically as

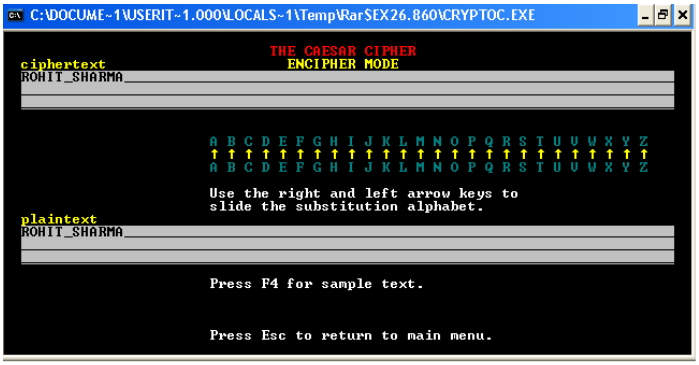
$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

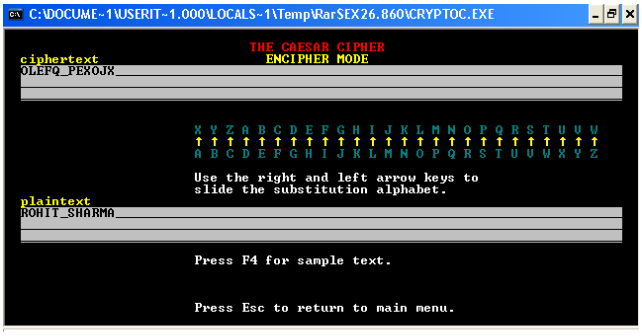
$$D_n(x) = (x - n) \mod 26.$$

In the above, 0...25 is the range for the result. I.e., when x+n or x-n are not in the range for the result, then we have to perform subtraction or addition of 26 [6].

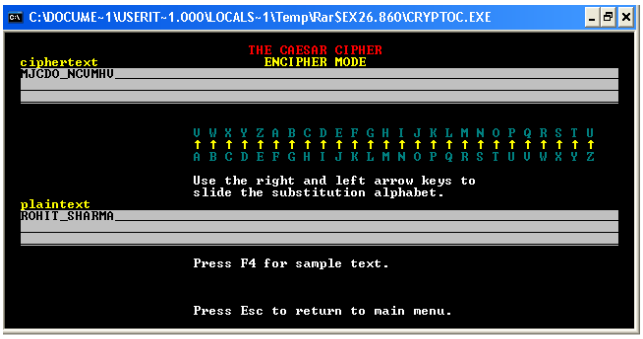
II.i- Encryption (fig-1)



With No Shifting



WITH THREE SHIFTING



WITH FIVE SHIFTING

II.ii- Security

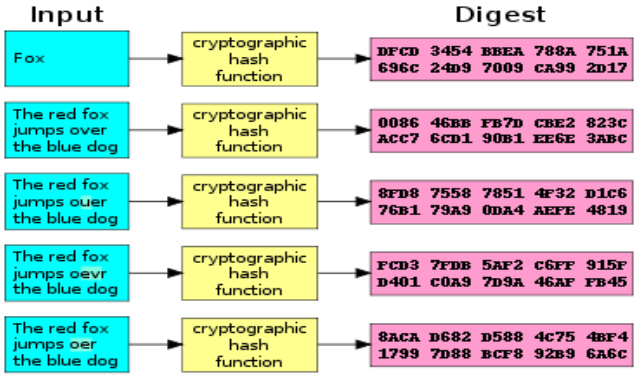
Results	
Original text	ROHIT SHARMA
Original bytes	52:4f:48:49:54:20:53:48:41:52:4d:41 (length=12)
Adler32	16590363
CRC32	e5ad3564
Haval	2a208ce22f7fa31e665a2f00a562159e
MD2	146fdaa2deb0c67c14d9130cadbb0a52
MD4	3c96085419b6ba588f3c15ade6382df2
MD5	655b613c0361ad2a6838600048345a69
RipeMD 128	8eb9c853a2c720a7f85c3a84ea0d52c3
RipeMD 160	d6f71e17bced95b75155b54cafe617 afadd74224
SHA-1	1c7389ed04a8a6d65e92d9a0a71571a8405 184f7

The key length is identical to the size of the given alphabet. Using the capital letters A-Z as alphabet allows 26 different keys, with the 26th key rendered meaningless because it would map each letter to itself. We have only 25 meaningful keys, it is quite easy to found correct one from all possible keys (brute-force analysis). The Caesar cipher can also easily be cracked with a frequency-analysis. [10] This talk will proposed a new technique that based on combination of techniques substitution and transposition. To make a cipher text that is not easy to crack, we have to Combining Caesar cipher with cryptographic hash function technique.[7][8]

III. Digestion

After the encryption we fed the data for digestion. Digestion can be performed by any of hashing techniques. A fixed size bit string can be return by an arbitrary block of data by using cryptographic hash, the *hash value*, any (accidental or intentional) change to the data can (with very high probability) change the hash value. The ability of Hash function must be to process an arbitrary-length message into a fixed-length output. For achieving that the input data should be broken into a series of equal-sized blocks, and used one-way compression function to operate them in sequence. This compression function can be specially designed for hashing or built from a block cipher.

Table-1



Merkle–Damgård construction hash function is compression function and it is resistant to collisions as it is compression function; in the compression function any collision can be traced back to a collision.

III-i- Examples of Data Digestion

String hash; ROHIT SHARMA

Table -2

A lot of cryptographic hash functions we have, but many of them should not be used due to found to be vulnerable. [5] We show the digestion of string ROHIT SHARMA by many hash functions methods. Mostly we used SHA-1 and MD5 hash functions.

IV. Application

Caesar cipher secured by "Hash Function" has some advantages over simple Caesar cipher.

- Difficult cryptanalyze.
- Reconstruction of result is not easy.
- Caesar cipher code cannot crack by Brute force attack.
- Overcome all the drawbacks of Caesar cipher.

Vi. Conclusion

Caesar cipher known as simplest substitution method. It is not very strong cipher. Main advantage is that it is simple and can be understand easily. The above advantage can have a problem of easy detection. This problem can be overcome by combining Caesar cipher with transposition techniques. Hashing is used as a Digestion technique here.

To increase complexity, stacks are used by which detection of both techniques (Caesar cipher and hashing) can make difficult. The proposed method is a combination of transposition and digestion hence it will give better security for transition in RFID security. However, the algorithms can be more improved to get better results.

ACKNOWLEDGMENT

I would like to give my sincere thanks to my guide Dr. P.K.Singh who helped and guided me throughout this paper.

.

REFERENCES

[1] Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill.
[2] ISO: ISO/EIC 14443, proximity cards (PICCs). Technical report, ISO (2006)
[3] William Stalling "Network Security Essentials(Applications and Standards)",Pearson Education,2004
[4] Symmetric Key Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: "Proceedings of International conference on security and management(SAM'10" held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).
[5] A new Symmetric key Cryptography Algorithm using extended MSA method :DJSA symmetric key algorithm, Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June,2011, Page-89-94.
[6] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: Neeraj Khanna,Joel James,Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath : Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130.
[7] Cryptography and Network, Willian Stallings, Prentice Hall of India.
[8] Cryptography & Network Security, B.A.Forouzan,;Tata-Mcgraw Hill Book Company
[9] Peter Montgomery, "Modular Multiplication Without Trial Division," Math. Computation, Vol. 44, pp. 519–521, 1985.
[10] Vinod Saroha1, Suman Mor2, and Anurag Dagar3," Enhancing Security of Caesar Cipher by Double Columnar Transposition Method", International Journal of Advanced Research in Computer Science and Software Engineering 1 (8), August- 2012, pp. 1-6.
[11] Gurdev Singh, Jimmy Singla and Shivdev Singh, "Message Encryption and Decryption" VSRD-IJCSIT, Vol. 2 (7), 2012, 668- 671.

Rohit sharma
Research scholar
Teerthankar Mahaveer University
Moradabad
E.mail: *rohit_techelectro@yahoo.com*

Dr.P.K.Singh
Prof. & Dean Academics
IIMT IET Meerut

E.mail: *pksingh0069@gmail.com*