Unassailable Cryptosystem for Securing Magnetic Stripe Card using A Brand New Hash and Encryption Algorithm

[1]**Latha Karthigaa.M.** [2] **Balachandar.N.** [2] **Karthi.M.**

[1]Lecturer, IT Department
[2] UG Students (III – B.E., - CSE)
Velalar College of Engineering and Technology, Erode–638012, Tamil Nadu, India.

Summary
In day to day life, Magnetic stripe card plays an important role. Open your wallet! See at least 10 to 15 cards in it. Wondering? Today, the world is fully in the hands of stripe cards since it is easy to carry and even if it is stolen, it is secure. But due to the increase in hackers today, Magnetic stripe cards are becoming insecure now. Even the Encrypted PIN can be easily stolen by the cryptanalysts. So it is time now to secure the Magnetic stripe card. In this paper, we have applied a new encryption and a new hash algorithm to keep the information secure in stripe cards. The main advantage of this paper is, on an average, even the supercomputer will take 10574 years to decrypt, which is 22.8% higher than the previous proposals.

Key words:
Brand New Hash, Encryption Algorithm.

Literature Review:

The normal encryption uses only English alphabets and it will have only 26! Combinations and can be easily decrypted. Furthermore, even usage of any ASCII characters or special characters will have fewer combinations for brute force attack and can be decrypted within certain period of time. By using the relative frequency, it is common to decrypt. To avoid various attacks like dictionary attack, mathematical attack, timing attack etc., we need an efficient way to encrypt the PIN in magnetic stripe cards.

Proposed Model:

Our proposed model is shown in the figure:1. Whenever a PIN number is assigned for a person, we have to transfer his PIN in an encrypted form to his Magnetic stripe card. The first step is to compute the hash value of the PIN. Now encrypt the PIN along with hash value. Thus, we obtained the encrypted PIN and it has to be transferred into the Magnetic stripe card.

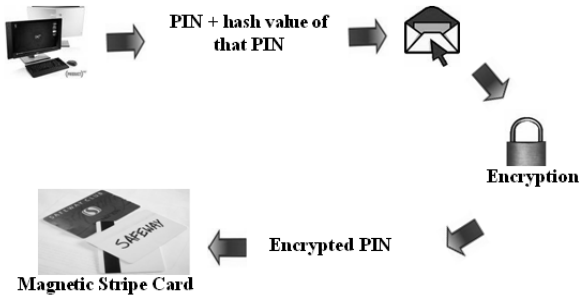

Figure 1: Proposed Model

This will improve the security in various ways. PIN is the important information which has to be more confidential while having any transaction. So, it should be kept in mind for preparing this model.

Proposed Hash Algorithm:

Before moving to the new one, we should know about the basic working principle of hash algorithm.

Working Principle of Hash Algorithm:

The input to the hash algorithm can be of any length. But output will be only of fixed length. It has to undergo various iterations of operations to obtain the fixed length of hash value [1]. There are various steps involved to bring the hash value into reality and security.

Advantages of Hash Algorithm:

The main advantage of the hash algorithm is “Collision Resistance”. That is, it is rare that two messages (in our case, it is PIN) have the same hash value, hence, making this algorithm a very grand success. Still it is “One way”

Manuscript received April 5, 2009
Manuscript revised April 20, 2009

and it is highly impossible for any cracker or hacker to break this algorithm.
Let us now discuss about some of the problems which is existing in the current day trends of the hash algorithm. The problem should be because of some flaws in the design of those algorithms.

Insecurity in Current SHA:

We should be known about the important thing that SHA 1 is broken and SHA 2 is about to be broken. That's why the NIST had called for new design of a brand new hash algorithm. Thus this is currently required.

Disadvantages of SHA Family:

- SHA family algorithms are relatively slower, due to large number of computations and operations.
- The initial value chosen by this hash algorithm is not dynamic, which is obviously known to all people especially to the people who love to hack.
- SHA family uses the **Merkle-Damgard model**, which leads to the length extension attack which in turn leads to insecure applications.
- It uses the static retriever table to initialize the values in all iteration of the hash algorithm and also to initialize the intermediate values.

Solutions to Overcome The Above Disadvantages:

- To make the system fast, we should reduce the number of operations. The second way to make it fast is by using the one way function that is, irreversible functions.
    - It is being recommended to use "Modulo" functions to perform irreversible operations.
- We should avoid using the static initial hash values. Use dynamic ones, using pseudo random generator or Blum-blum shub (BBS) generator.
- Instead of using Merkle-Damgard model, we are using a different construct called as "Unassailable Construct" which avoids the length extension attack.
- We use a dynamic retriever keyed/unkeyed algorithm for more efficiency.

Proposed Unassailable Cryptosystem:

There must be an algorithm where the above disadvantages should be avoided. So we put forth our whole effort to develop a new algorithm for Information security. We used an algorithm named **'n' level UNICODE- position- character- length ciphers**. Here the total characters used for encryption is 255 and the number of alternate keys are nearly $\mathbf{2.85*10}^{511}$.
Here it used UNICODE characters instead of English alphabets. Since it used the position value, the relative frequency attack is being avoided.

Introduction:

The **DATE** and **TIME** on which the user obtained the Magnetic stripe card is the important key for the particular customer. It is hard for the hackers to decrypt the data. Since the encryption and decryption involves position, length of the plain text along with the **UNICODE** value of the character, it may be greatly used in the future to give high performance. This is implemented in 'n' levels where n=1, 2, 3… and hence it is called as 'n' level **UNICODE** position – character - length ciphers. Level of encryption is given to the destination in prior and 'n' levels made our algorithm even more secure. As long as the level and length of the PIN is high, it is hard for the cryptanalyst to hack the PIN.

Plain Text: DATE & TIME + PIN.

This is the plain text for our algorithm, which is further taken for encryption. This will bring out the largest performance ever heard. Hence it is recommended for various applications and we are applying it in ATM machine.

Encryption:

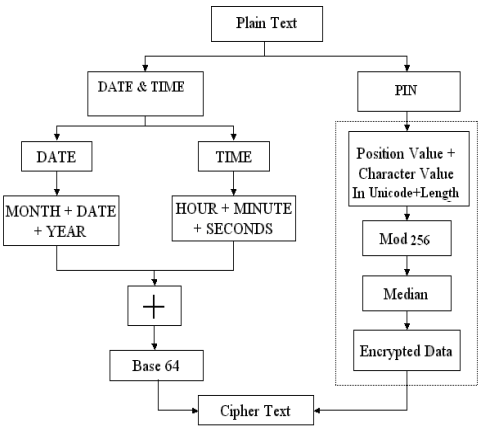

Figure 2: Depiction of Encryption.

Explanation:

Initially the DATE is retrieved from the ORACLE database and the sum of date, month and year is calculated. Further, the TIME value is also retrieved and hour, minutes and seconds are summed up. Then sum up both date and time. Now the obtained value is subjected to BASE 64 computation and 'n' value is obtained. The algorithm gets executed 'n' times which is the output value of BASE 64. Then the cipher text is obtained. Median value should be computed and is padded at the end.
This algorithm will take less time for encryption and takes more time for hackers to decrypt. This highly supports day to-day life's activities.

Encryption:

In the network environment, the security is maintained by using the User Name and the PIN. First database shows the User name, PIN in encrypted form and DATE & TIME in encrypted form. The encryption for PIN involves the above Encryption formula and the encryption for DATE & TIME involves some random Encryption algorithms. In the second database, Username with DATE & TIME are stored. It is the efficient way to store PIN in the distributed environment.

Implementating Ciphers:

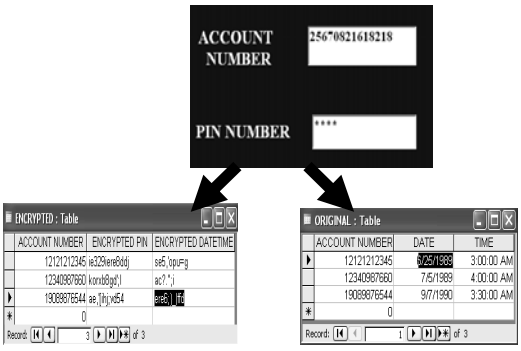

Figure 3: Maintenance of database

Decryption:

When a person is entering his/her PIN to login, his/her PIN in encrypted form is decrypted with DATE & TIME (on which customer registered) in the second database and compares it with the currently typed one. Thus in this proposal, the PIN is saved nowhere, enhancing the efficiency of the proposal.

Encryption Formula:

Then the cipher text can be calculated by using the formula,

- Cipher text= (position value of the character + character value in UNICODE + Total length of the plain text) mod 255.
- Find the median of the obtained cipher text and pad it at the end.
- Find the base 64 value of the system's DATE & TIME and it at first.

Advantages of 'n' Level Position-Character-Length Ciphers:

- It involves 'n' levels of encryption and it is hard for the cryptanalysts to hack the password where n=1, 2, 3….
- Since the cipher text what we have used is UNICODE and there is nearly 256 combinations available and is hard for the hackers.
- Even the relative frequency of occurrence of data will not help the cryptanalysts because the position of the plain text is used to convert into cipher text.

Complexity Analysis:

- **Number of alternate keys**
  $= 2^{256} * 255! * 10^{6} * 2 * 4$
  $= 3.082 * 10^{588}$ keys.
- **Number of keys that can be found in a day at 1 decryption/μs**
  $= 24 * 60 * 60 * 10^{6}$
  $= 8.64 * 10^{10}$ keys decrypted/Day
- **Number of keys that can be found in a year at 1 decryption/μs**
  $= 8.64 * 10^{10} * 365$
  $= 3.15 * 10^{13}$ keys decrypted/year
- **Number of years required to find the key at 1 decryption/μs**
  $$= \frac{3.082 * 10^{588}}{3.15 * 10^{13}}$$
  $= 9.784 * 10^{574}$ years.

Deploying in Magnetic Stripe Card:

Now, we have got the encrypted PIN. That has to be transferred into the magnetic stripe card. For that we use a magnetic stripe writer. The magnetic stripe card consists of magnet at the back which is used for storing information. That information is very confidential, and is illegal for a person to write it without any authority. Many crackers are using the magnetic stripe writer illegally. We should take into account that the information present in the card is unreadable for a hacker.

Magnetic Stripe Card:

A **magnetic stripe card** is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called a **magstripe**, is read by physical contact and swiping past a reading head. Magnetic stripe cards are commonly used in credit cards, identity cards, and transportation tickets. They may also contain an RFID tag, a transponder device and/or a microchip mostly used for business premises access control or electronic payment.
In most magnetic stripe cards, the magnetic stripe is contained in a plastic-like film. The magnetic stripe is located 0.223 inches (5.66 mm) from the edge of the card, and is 0.375 inches (9.52 mm) wide. The magnetic stripe contains three tracks, each 0.110 inches (2.79 mm) wide. Tracks one and three are typically recorded at 210 bits per inch (8.27 bits per mm), while track two typically has a recording density of 75 bits per inch (2.95 bits per mm). Each track can either contain 7-bit alphanumeric characters, or 5-bit numeric characters. Track 1 standards were created by the airlines industry (IATA). Track 2 standards were created by the banking industry (ABA). Track 3 standards were created by the Thrift-Savings industry. Magstripes following these specifications can typically be read by most point-of-sale hardware, which are simply generic general-purpose computers that can be programmed to perform specific tasks. Examples of cards adhering to these standards include ATM cards, bank cards (credit and debit cards including VISA and MasterCard), gift cards, loyalty cards, driver's licenses, telephone calling cards, membership cards, electronic benefit transfer cards (e.g. food stamps), and nearly any application in which value or secure information is *not* stored on the card itself. Many video game and amusement centers now use debit card systems based on magnetic stripe cards.

In our Project, we are using **track 2** for storing and retrieving information.

ATM Machine with The Central Database:

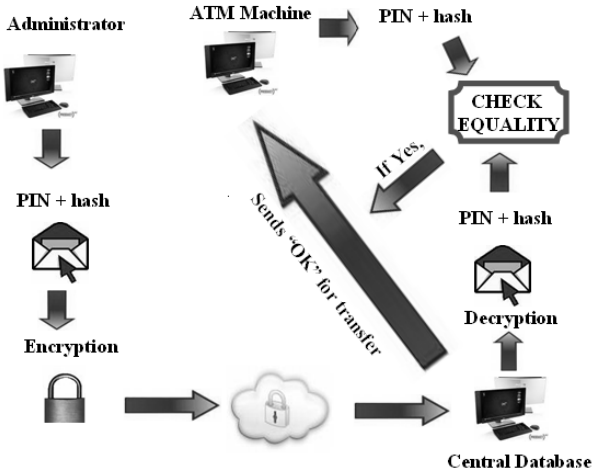

Figure 4: Proposed ATM application

Advantages of The Proposed Model:

The main advantages of this proposed set up are

- **Active attack** is avoided due to the usage of the brand new secure hash algorithm.
- **Passive attack** is avoided due to the usage of the brand new encryption and decryption algorithm.
- **Relative Frequency attack** is avoided due to the usage of the term "Length" (Length of PIN).
- **Brute Force attack** works less efficiently due to increase in number of combinations of keys.
- **Dictionary attack** is avoided due to the presence of "Median" operation in the encryption algorithm.
- **Number of combinations** in the cipher text of computed PIN increases due to the usage of "BASE 64" computation.

Conclusion:

Thus this cipher is used in the encryption algorithm, which gave high performance. So it is now highly easy to store the information like PIN in the magnetic stripe card safely.

Future Enhancements:

The PIN management is presently done in single encryption and single decryption. In future, it can be implemented in dual encryption and dual decryption. It can also be developed as a PIN management format or any other confidential information wherein we apply dual encryption and a single decryption. This dual encryption may increase the key complexity and reduce the users' complexity. This may require higher hardware requirements.

References

[1] Specifications for secure hash standard: http://www.csrc.nist.gov/publications/
[2] Requirements for SHA-3: http://www.nist.gov/hash-competition.
[3] "Cryptography and network security – Principles and practices" by William Stallings, Third Edition.

Latha Karthigaa.M had completed B.Tech (IT) in Velalar College of Engineering and Technology and she had secured **University 2nd rank** in Anna University, Chennai. She was the "**Best Outgoing Student Award**" winner of the academic year 2007-08. Now, she is currently working as a Lecturer in Velalar College of Engg & Tech.

Balachandar.N, pursuing his Third year Bachelor of Computer Science and Engineering in Velalar College of Engineering and Technology, Erode-12, Tamil Nadu, India. He got certified from Microsoft as **Microsoft Certified Professional** (MCP) on Managing and Maintaining a Microsoft Windows Server 2003 Environment with 94%.

Karthi.M, pursuing his third year B.E (Computer Science and Engineering) in Velalar College of Engineering and Technology, Erode-9, Tamil Nadu, India. He is interested in programming, cryptographic algorithms for Cryptography, Computer and Network Security.