DESIGN OF AN ALGORITHM TO ENCRYPTION PATTERN LOCK THROUGH MD5

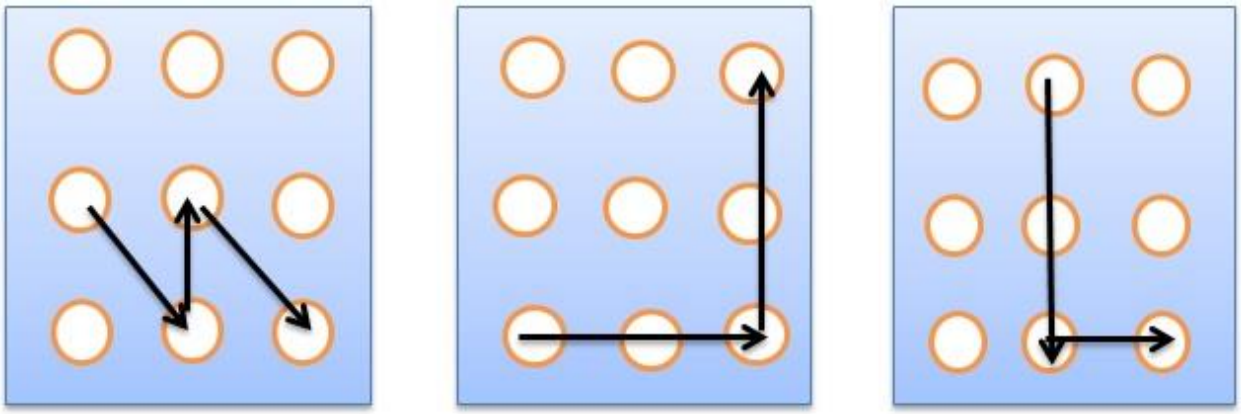
Pawan kumar, kanika, Beer singh, Dr.Alka,
Student (M.Tech Software Engineering), P.h.d scholar, Student (M.Tech Software Engineering), Assistant professor
Department of Information Technology (M.Tech Software Engineering),
Babasaheb Bhimrao Ambedkar University Vidya Vihar Lucknow India

ABSTRACT:-
Now a day every system to introduce to the touch screen and all users have some confidential information like a business meeting, financial statement, private message and many more which are want to secure to another person. Every user wants to secure confidential information and fast processing. In this paper, we are introduced to pattern lock with MD5 algorithm technique which is faster than another encryption technique.

Keywords:-
Encryption, Password, MD5, SHA1, Pattern lock, Touchscreen, and Algorithm.

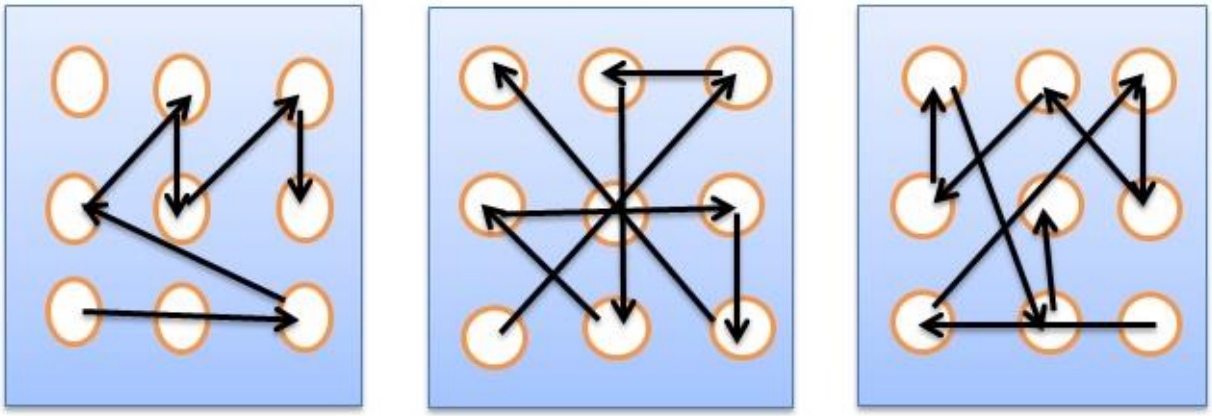
INTRODUCTION

Message Digest 5 (MD-5) is a standout amongst the most broadly utilized of one-way hash function. MD-5 is the fifth hash work outlined by Ron Rivest. MD-5 is an improvement of MD-4 where there is an expansion of one round. MD-5 forms the info content into 512 piece bits of blocks, isolated into 32 bits of sub-block of 16 pieces. The yield of the MD-5 is 4 pieces of 32 bits every which will be the typical 128 bits called the hash value. MD5's primary hub has a 512 piece long message obstruct that goes into 4 rounds. The yield of MD-5 is 128 bits from the most lowest byte A and the highest byte D Each message will be encoded, first searched what number of bits are contained in the message[1]. As per RFC 1321 "MD5 message process calculation takes as information a message of discretionary length and process as yield a 128-bit Fingerprint or message process of the output"[3, 4].MD5 is the contraction of Message-Digest Algorithm 5, which was created mutually by MIT Computer Science Research facility and Ronald L. Rivest from RSA Data Security Inc. in the mid-90s in the twentieth century and advanced from MD2, MD3, and MD4. It packs a snippet of data with plain code and arbitrary length into 128 bits esteem by hash calculation, which is called data occupy. The MD5 calculation is irreversible and can't recoup the first plain code data from data reflection, therefore it is constantly trusted safe. This exposition examines the utilization of MD5 calculation in secret key validation and its security, and tests into the physical measures of the application security of MD5 calculation in secret word verification [2, 3, 4].Pattern locks use 9 dots to lock the device. This is a very popular method in the present time. Pattern lock very to use than text password and now a day most of the systems are a touch screen so a lot of users use pattern lock now a day. Some examples of simple pattern lock and complex pattern lock are shown in figure-1and figure-2 respectively.



[A] [B] [C]

Figure 1: An example of simple pattern.



[A] [B] [C]

Figure 2: An example of a complex pattern.

In the above figures defined simple and complex pattern lock. If we are used approximate all the dots then this make complex pattern lock and if we used less number of dots then this becomes simple pattern lock.

In the figure 1, [A] figure has 4->8->5->9, [B] figure has 7->8->9->6->3 and [C] figure has 2->5->8->9 pattern lock password which is simple type password.

In the figure 2, [A] figure has 7->8->9->4->2->5->3->6, [B] figure has 7->5->3->2->5->8->4->5->6->9->5->1 and [C] figure has 9->8->7->5->3->6->2->4->1->8->5 pattern lock password which is complex type password.

I. Related work:-

Text-based passwords and PIN codes are typically coupled with financial balances, computational gadgets and so forth. People gangs a few records and various passwords that need to recall. Along these lines, the clients regularly need to adjust ease of use with security. As an outcome, they may review another record's secret word or far more terrible utilize the same over the entirety of their records [9, 10]. Specialists have additionally recommended the utilization of graphical passwords as a less demanding other option to text passwords, in light of individuals have a superior capacity to review pictures than text. Distinctive ease of use thinks about have laid out the favorable circumstances of graphical passwords, for example, their sensible login and creation times, worthy mistake rates, great general observation and decreased obstruction contrasted with text passwords, yet additionally their vulnerabilities. As mention earlier, pattern locks are one type of recall based password based on graphics [9, 10]. The sha1 encryption method is used in the current time pattern lock scenario. This sha1 is slow processing so that why we used MD5 method for encryption in pattern lock [11].

II. Research Method:-

Pattern lock with MD5:

[1]. Flowchart:-

In the figure:-3 we discussing that how will work MD5 with pattern lock. In above figure that is clearly mention that taking input from the touch screen and its store in the variable like initial, middle and final variable name. Middle value takes an array which can store more than one value. Then all variable value stored in an array with arbitrary length. After storing the value in the array it will be given to MD5 function for fingerprint or message digest.

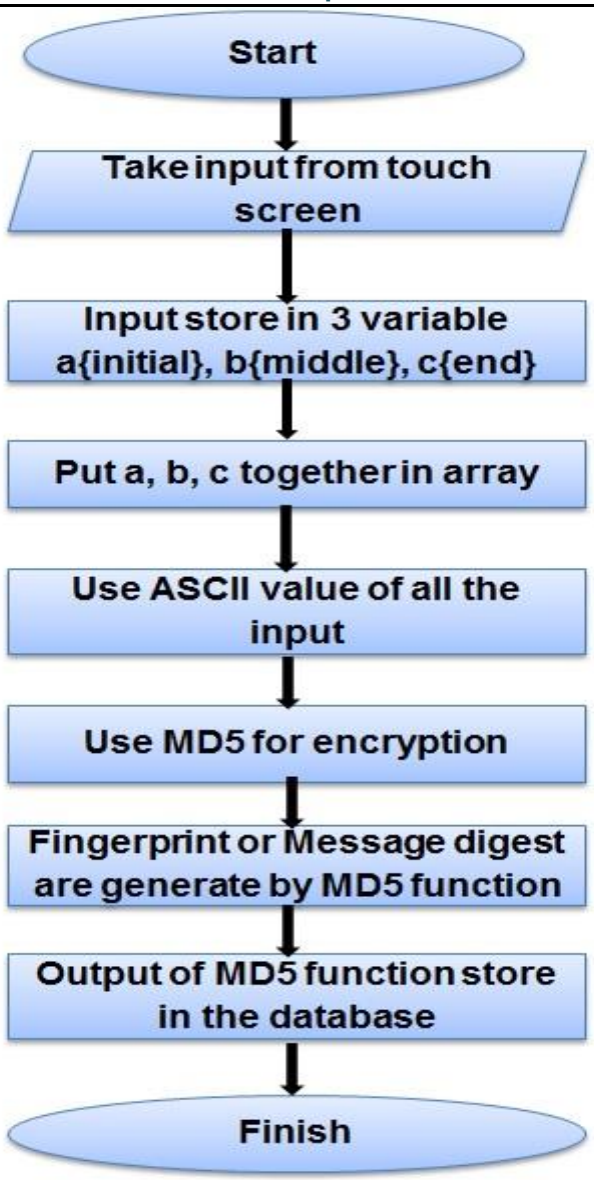


Figure 3: - Flowchart of pattern lock with MD5.

Value storing and processing with MD5 function:-

Firstly take the three variable, the first variable take an initial value of pattern lock and second variable take middle value of the pattern lock its take an array which stores one or more value because of the middle (intermediate) and last variable is final point that means ending point of pattern lock.

There are some examples of pattern lock with variable storing for processing md5.

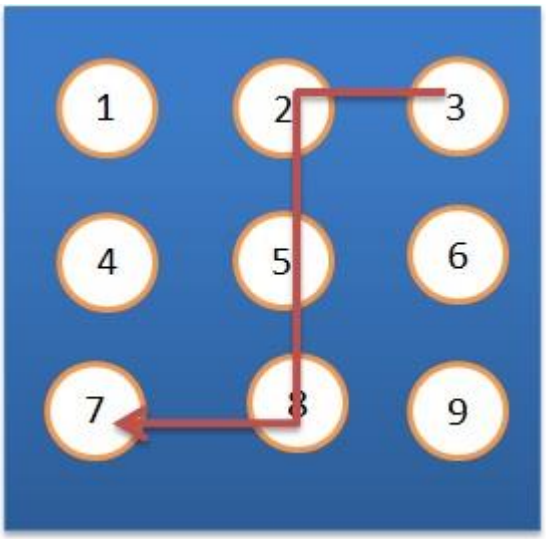


Figure 4: An example of pattern lock.

In the above figure

Starting or initial value A = 3

Middle value B[] ={2, 5, 8 }

Finale value C = 7

These value stored in the array like in the same sequence.

Initial value A = 3	Middle value B[] ={2, 5, 8}	Finale value C= 7
[0]	[1]	[2]

Store with the value:-

The actual value stored in the array.

3	2	5	8	7
[0]	[1]	[2]	[3]	[4]

These value store in the array and send to the MD5 function for message digest.

Now working with MD5:-

3	2	5	8	7	……..	512bits
[0]	[1]	[2]	[3]	[4]	……[511]	

ASCII value of 3, 2, 5, 8, 7 respectively is 51, 50, 53, 56, 55. Which store in the array.

Appending padding bits:-

51	50	53	56	55	1	.....	…….	0	0
[0]	[1]	[2]	[3]	[4]	[5]	…..	… …..		[511]

Initialize MD Buffer:-

A four-word buffer (O, P, Q, R) is used to compute the message digest. Here each of O, P, Q, R is a 32-bit register. These registers are initialized to the following values in hexadecimal, low order bytes first):

word O: 01 23 45 67
word P: 89 ab cd ef
word Q: fe dc ba 98
word R: 76 54 32 10

Process Message in 16-Word Blocks:-

We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

F(A,B,C) = AB v not(A)C
G(A,B,C) = AC v B not(C)
H(A,B,C) = A xor B xor C
I(A,B,C) = B xor (A v not(C))

v denotes:- OR logic gates
xor denotes:- XOR logic gates
not denotes :- NOT logic gates
Do the following:

```
/* Process each 16-word block. */
For i = 0 to N/16-1 do
/* Copy block i into X. */
  For j = 0 to 15 do
Set X[j] to M[i*16+j].
end  /* of loop on j */

    /* Save O as OO, P as PP, Q as QQ, and R as RR. */
  OO = O
  PP = P
  QQ = Q
  RR = R

  /* Round 1. */
  /* Let [opqr k s i] denote the operation o = p + ((o + F(p,q,r) + X[k] + T[i]) <<< s). */
```

/* Do the following 16 operations. */
[OPQR 0 7 1] [ROPQ 1 12 2] [QROP 2 17 3] [PQRO 3 22 4]
[OPQR 4 7 5] [ROPQ 5 12 6] [QROP 6 17 7] [PQRO 7 22 8]
[OPQR 8 7 9] [ROPQ 9 12 10] [QROP 10 17 11] [PQRO 11 22 12]
[OPQR 12 7 13] [ROPQ 13 12 14] [QROP 14 17 15] [PQRO 15 22 16]

/* Round 2. */
/* Let [opqr k s i] denote the operation o = p + ((o + G(p,q,r) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[OPQR 1 5 17] [ROPQ 6 9 18] [QROP 11 14 19] [PQRO 0 20 20]
[OPQR 5 5 21] [ROPQ 10 9 22] [QROP 15 14 23] [PQRO 4 20 24]
[OPQR 9 5 25] [ROPQ 14 9 26] [QROP 3 14 27] [PQRO 8 20 28]
[OPQR 13 5 29] [ROPQ 2 9 30] [QROP 7 14 31] [PQRO 12 20 32]

/* Round 3. */
/* Let [opqr k s t] denote the operation o = p + ((p + H(p,q,r) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[OPQR 5 4 33] [ROPQ 8 11 34] [QROP 11 16 35] [PQRO 14 23 36]
[OPQR 1 4 37] [ROPQ 4 11 38] [QROP 7 16 39] [PQRO 10 23 40]
[OPQR 13 4 41] [ROPQ 0 11 42] [QROP 3 16 43] [PQRO 6 23 44]
[OPQR 9 4 45] [ROPQ 12 11 46] [QROP 15 16 47] [PQRO 2 23 48]

/* Round 4. */
/* Let [opqr k s t] denote the operation o= p + ((o + I(p,q,r) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[OPQR 0 6 49] [ROPQ 7 10 50] [QROP 14 15 51] [PQRO 5 21 52]
[OPQR 12 6 53] [ROPQ 3 10 54] [QROP 10 15 55] [PQRO 1 21 56]
[OPQR 8 6 57] [ROPQ 15 10 58] [QROP 6 15 59] [PQRO 13 21 60]
[OPQR 4 6 61] [ROPQ 11 10 62] [QROP 2 15 63] [PQRO 9 21 64]

/* Then perform the following additions. (That is increment each of the four registers by the value it had before this block was started.) */
O = O + OO
P = P + PP
Q = Q + QQ
R = R + RR
end /* of loop on i */

Output:-

The message digest produced as output is A, B, C, D. That is, we begin with the low-order byte of A, and end with the high-order byte of D and store to the database in the system [3, 4].

Example :-

Pattern lock is 3->2->5->8->7. This is pattern lock text and this is encrypted then value is 0bb08463277724510 45bd30dd347821b. Pattern lock is minute change like 3->2->5->8 then md5 encryption value is 485843481a7edacbfce101ecb1e4d2a8 [7].

[2]. Block diagram:-

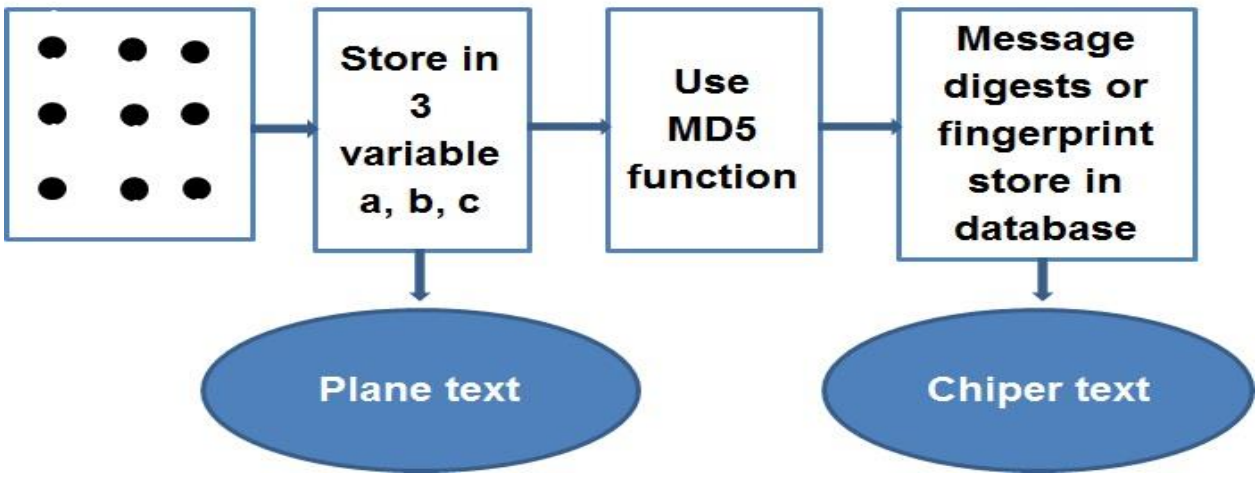


Figure 5:- Block diagram of pattern lock with MD5.

In figure 5, this is a block diagram of pattern lock with the MD5 working process. In this block diagram, we are showing taken the input as plane text then stores in the variables, this plane text given to the MD5 function for message digest or fingerprint (chiper text).

III. CONCLUSIONS AND FUTURE WORK:-

MD5 generates a 128-bit long message digest. This is faster than any another method because of its takes only 64 iterations are required. To attack required to find out original message need 2^128 bit operation are required. If use MD5 with pattern lock then locking and the unlocking system goes fast compare to another method. Pattern locks provide 9 dots combination. If your maximum number of dots are used then become harder to break the password. The MD5 method is faster as well as secure other than encryption method. This method can use in future with another method which is faster and more secure encryption method.

IV. References:-

1. Dhany H. et.al, "Encryption and Decryption using Password Based Encryption, MD5, and DES", International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017), pp., 2017.
2. Zheng X, Jin J. Research for the application and safety of MD5 algorithm in password authentication. InFuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on 2012 May 29 (pp. 2216-2219). IEEE.
3. THE MD5 Message-Digest Algorithm at https://tools.ietf.org/html/rfc1321
4. R. Rivest MIT Laboratory for Computer Science and RSA Data Security, Inc April 1992 at http://www.rfc-editor.org/rfc/rfc1321.txt
5. ASCII codes table at https://ascii.cl/
6. Andriotis P, Tryfonas T, Oikonomou G, Yildiz C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. InProceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks 2013 Apr 17 (pp. 1-6). ACM.
7. MD5 online, https://www.md5online.org/md5-encrypt.html
8. MD5 Algorithm Description with an example at https://www.scribd.com/doc/35954574/MD5-With-Example.
9. Andriotis P, Tryfonas T, Oikonomou G, Yildiz C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. InProceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks 2013 Apr 17 (pp. 1-6). ACM.
10. Angulo J, Wästlund E. Exploring touch-screen biometrics for user identification on smart phones. InIFIP PrimeLife International Summer School on Privacy and Identity Management for Life 2011 Sep 5 (pp. 130-143). Springer, Berlin, Heidelberg.
11. Padma MB, Kumar MG. Design And Analysis of An Enhanced SHA-1 Hash Generation Scheme for Android Mobile Computers. International Journal of Applied Engineering Research. 2016;11(4):2359-63.
12. Padma B, Raj Kumar GV. A review on android authentication system vulnerabilities. International Journal of Modern Trends in Engineering and Research (IJMTER). 2016;3(8):118-23.
13. Padma B, RAJKUMAR GS. PREVENTING SECURITY ATTACKS ON MOBILE PATTERN PASSWORDS. Journal of Theoretical & Applied Information Technology. 2018 Feb 28;96(4).
14. Gupta S, Goyal N, Aggarwal K. A review of comparative study of md5 and ssh security algorithm. International Journal of Computer Applications. 2014 Jan 1;104(14).
15. Järvinen KU, Tommiska M, Skyttä J. A Compact MD5 and SHA-1 Co-Implementation Utilizing Algorithm Similarities. InERSA 2005 Jun (pp. 48-54).