Securing Student Marks Using Sea Encryption Algorithm

M.Mounika[1], Mr.G.Ananthnath[2]
[1]*Student, Dept. of MCA, KMM Institute of Post Graduate Studies*
[2] *Asst. Professor, Dept. of MCA, KMM Institute of Post Graduate Studies*

***Abstract*- Security means protect the information with different systems from unauthorized persons. Cryptography is one of the technique,it is used to secure or protect the information from systems through encryption and decryption algorithms. In proposed system we are used Sea Encryption algorithm. By this algorithm we secure the student marks. The method of sea encryption set of rules is to accepts the actual text content(A) and key (ok) for encryption and it divide both the actual textual content and key in one-of-a-kind procedure. Decryption process can done by code sheet. Code sheet having input code, print code and accept code. It provides less complexity and improve their performance and security is high.**

***Index Terms*- Encryption, Decryption, SeA encryption algorithm, Information Security.**

I. INTRODUCTION

Sea Encryption Algorithm is mainly two strategies that are AES, DES. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the authorities to protect categorised information and is applied in software and hardware throughout the world to encrypt sensitive records. The national Institute of standards and generation (NIST) started out improvement of AES in 1997 whilst it introduced the need for a successor set of rules for the records Encryption standard (DES), which become beginning to come to be liable to brute-force attacks. AES features are security, cost, implementation.

Security: Competing algorithms have been to be judged on their capability to withstand attack, as compared to different submitted ciphers, although protection energy was to be considered the most important aspect within the opposition.

Cost: Intended to be launched beneath a worldwide, nonexclusive and royalty-unfastened basis, the candidate algorithms had been to be evaluated on computational and reminiscence efficiency.

Implementation: algorithm and implementation traits to be evaluated blanketed the ability of the set of rules; suitability of the set of rules to be carried out in hardware or software; and usual, relative simplicity of implementation.

The Data Encryption Standard(DES) is a symmetric-key set of rules for encryption of digital statistics. even though now taken into consideration insecure, it became tremendously influential within the advancement of present day cryptography. Cryptography is the exercise and look at of techniques for communication within the presence of 0.33 events called adversaries. more normally, cryptography is set building and studying protocols that save you third events or the general public from analyzing non-public messages; various factors in information safety which include records confidentiality, information integrity, authentication, and non-repudiation are valuable to fashionable cryptography. contemporary cryptography exists at the intersection of the disciplines of mathematics, laptop science, electric engineering, conversation technological know-how, and physics. programs of cryptography encompass electronic commerce, chip-primarily based fee cards, virtual currencies, pc passwords, and army communications.

The Data Encryption Standard(DES) is a symmetric-key set of guidelines for encryption of digital records. despite the fact that now considered insecure, it became incredibly influential inside the advancement of contemporary cryptography. Most people from reading 255fb4167996c4956836e74441cbd507 messages; different factors in information protection which consist of statistics confidentiality, information integrity, authentication, and non-repudiation are

precious to modern cryptography. current cryptography exists at the intersection of the disciplines of arithmetic, pc science, electric powered engineering, verbal exchange technological bdd5b54adb3c84011c7516ef3ab47e54, and physics. programs of cryptography encompass electronic commerce, chip-primarily based fee cards, virtual currencies, pc passwords, and military communications.

Code Sheet contains three types of codes

1. Input code (IC)
2. Print code (PC)
3. Accept code (AC)

1. *Input Code*- The input of each character is entered by pressing "ALT+along with its corresponding number ".

2. *Print Code*- If the input for letter 'a' is given the corresponding another character will be printed on to the screen.

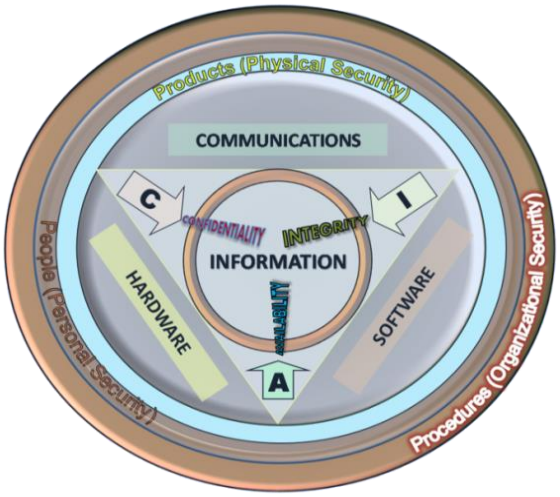
3. *Accept Code*- If the input for letter 'a' is given the memory will accept the letter 'a' whereas print another character on the monitor screen so that third person intrusion are avoided.

II. RELATED WORK

Information: data and information are often used as if they are the same. Technically, information can be defined as the data which have been processed to a meaningful end. Information Security: this means protecting information and information systems from unauthorized access, disruption, modification, inspection, recording or destruction. Vulnerability: this is the weakness that could be used to endanger or cause harm to an informational asset[11].

III. SEA ENCRYPTION ALGORITHM

The main domain of the algorithm is for information security. The algorithm satisfies all the four objectives of cryptography. They are, Confidentiality, Integrity, Non-repudiation, Authentication.The process of sea encryption set of rules is to accepts the actual text content (A) and key (ok) for encryption and it divide each the actual textual content and key in different method.



In this algorithm encryption and decryption are seperatly. for encryption process, it accepts the actual text content(A) and key (ok) for encryption and it divide both the actual textual content and key in different method.For decryption process, can be done by using the code sheet, which includes three types of code namely the Accept code, Print code and the Input code. The decrypted data can be viewed by the receiver if the person knows the key and the code sheet design.

Encryption:

The encryption process in SeA set of rules uses simple methodology. The encryption method is as follows,

Methodology:

encryption process at first accepts the Actual Text from the sender.

b. The process is set in such a way that once it has accepted the actual text it will start generating the corresponding ASCII values for all the characters mentioned in the actual text.

c. According to binary search method, The ASCII values are divided into two and separated as processes as illustrated below:

The process P1 = {A1, An/2+1} is taken. First it will pass to the Position Table (mentioned below) that consists of alphabets and its shuffled values. The table contains 26 characters. Then the process continues which is similar to decryption process.

Code Sheet Design:

a. The Code Sheet is simply to accept the text through the respective numbers of each character when keyboard is locked.
b. The permutation and combination are applied on 66 characters on keyboard to design the Code Sheet Design[4].
c. In application, the Code Sheet consists of three types of code:
a) Input code (IC)
b) Print code (PC)
c) Accept code (AC)
d. The Code Sheet contains sixty six characters for each category as follows,
For example, The actual text (A) = "abc012……."

Input Code- The input of each character is entered by pressing "ALT + along with its corresponding number "

Print Code- If the input for letter 'a' is given the corresponding another character will be printed on to the screen.

Accept Code- If the input for letter 'a' is given the memory will accept the letter 'a' whereas print another character on the monitor screen so that third person intrusion are avoided.

Decryption:
The sea Encryption set of rules will refer Code Sheet first then it'll move for assessment of encrypted text (A) and key (ok) and ultimately it's going to pass for the technique (P). It accepts the Encrypted text(a) and key(ok) and defines the manner as,
A= { A1, A2 ,A3, …,An }
ok= { k1, k2 , k3 ,…, kn }
The procedure P is described as,
P={ P1, P2, P3 ,… , Pn n}
step one is increase the power of the key (okay) then compare A with ok. after that 3 options are furnished as
A is much less than ok (A
A is greater than K (A>okay)
A is same to ok(A=k)
This system is just like the binary search method the stairs are described within the following as:
1. If A > okay then, The process is based totally on A and described through P1 then test the circumstance till A = k.
2. If A < okay then,The system is primarily based on ok and defined via P2 then check the condition until A = ok.
3. If A =okay then, The manner (P) is based totally on each the P1& P2. the general manner is defined inside the following figure 2. (ii). when the set of rules meets the manner A, on the other hand it'll do the identical system. So the cipher text (C) , because C is primarily based on the range of comparisons of A and ok.

IV. CONCLUSION

In this system we are use sea encryption algorithm, In that we have four objectives, Confidentiality, Integrity, Non-repudiation, Authentication. And three modules, encryption, code sheet, decryption. Encryption method is used to secure student marks or information but it has less strength. By this algorithm, developing encrypting for the data of the key is strength and effective. It having code sheet, by this we can give any input, it must give correct input by this code sheet. For decryption method, increase the strength of the key (K) then compare A with K. Finally it give high key strength.

REFERENCES

[1] Basili, V., Heidrich, J., Lindvall, M., Münch, J., Seaman, C., Regardie, M., and Trendowicz, A. (2009). "Determining the impact of business strategies using principles from goal-oriented measurement." Proceedings of Wirtschaftsinformatik 2009: 9th International Conference on Business Informatics. Vienna. Available at http://www.dke.univie.ac.at/wi2009/Tagungsband_8f9643f/Band1.pdf
[2] Rostyslav Barabanov, Stewart Kowalski, Louise Yngström "Information Security Metrics: Research Directions".
[3] Quinn, S., Waltermire, D., Johnson, C., Scarfone, K., and Banghart., J. (2009). "The technical specification for the security content automation protocol" (Version 1.0). Gaithersburg, MD: National Institute of Standards and Technology.
[4] Dhillon, Gurpreet (2007). Principles Of Information Systems Security: text and cases.

NY: John Wiley & Sons. ISBN 978-0471450566.

[5] Layton, Timothy P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.

[6] Wang, L., Islam, T., Long, T., Singhal, A., and Jajodia, S. (2008). "An attack graphbased probabilistic security metric." Proceedings of DBSEC 2008: 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security. London, UK.

[7] Nasako Takashi, Murakami Yasuyuki, Kasahara Masao (2008). "IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E91-A Issue 10 (October 2008), pp.2833-2842. ISSN: 0916-8508".

[8] A. Vorster and L. Labuschagne, "A framework for comparing different information security risk analysis methodologies," University of Johannesburg, 2005.

[9] J. Aagedal, F. Den Braber, and K. Stolen, "Model-based risk assessment to improve enterprise security," http://coras.sourceforge.net/online_documentation.html, 2002.

[10] Z.Yazar, "A Qualitative Risk Analysis and Management Tool – CRAMM," SANS Institute InfoSec Reading Room, 2011.

[11] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.656.9659&rep=rep1&type=pdf