Int. J. Advanced Networking and Applications 29
Volume: 03 Issue: 05 Pages:29-35 (2012)
*Special Issue of NCETCSIT 2011 - Held on 16-17 Dec, 2011 in Bapurao Deshmukh College of Engineering, Sevagram*

# Strengthening of Data Security against its Attack

Swapnil G. Deshpande
Department of Computer Science, Vinayak Vidyamandir, Amravati,
swapnildeshpande33@gmail.com

Dr. Pradeep.B. Dahikar
Department of Electronics, Kamla Nehru College, Nagpur
pbdahikarns@rediffmail.com

***Abstract:-*** **This paper specifies cryptographic algorithm Hybridizing Traditional Technology (H.T.T) which may be used to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form.**
**The focus of the presentation will lie in presenting the symmetric and asymmetric algorithms, and specifics how it differs from each other.**
**We propose a new algorithm Hybridizing Traditional Technology (H.T.T) which enables us to demonstrate its security against all known types of attack. It is as fast as DES on the market leading Intel Pentium/MMX platforms (and at least as fast on many others); yet we believe it to be more secured than all other algorithms.**
**Use of this algorithm has improved the hardware complexity and the rate of encryption/decryption. Similarities of encryption and decryption are used to provide a high performance using an efficient architecture. The efficiency of the design is quite high due to use of short and balanced combinational paths in the design.**

**Keywords –** asymmetric key, authentication, cryptography, digital signature, hash function, symmetric key

## I. Introduction

Database management system maintains the integrity and confidentiality of data hence the need for Strengthening Data Security is growing. One of the necessities for securing databases is to encrypt the information stored inside them.
The hidden information is called “cipher text”. Converting plaintext to cipher text is performed by encryption while the procedure of converting the cipher text to plaintext is performed by decryption [1].
Cryptography is the science of using mathematics to encrypt and decrypt data. The Security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm also known as cipher and the secrecy of the key.
There are two major classes of encryption / decryption algorithms, which may be classed as Symmetric, or Conventional Cryptography and Asymmetric or Public Key Cryptography [2].
In symmetric encryption/decryption algorithms same key is used to encrypt and decrypt the file. The Data Encryption Standard (DES) and Substitution Cipher are example of conventional cryptography.
The "asymmetric" encryption/decryption algorithms use to decode the data is different to the key used to encode it. Asymmetric schemes are also commonly known as public key encryption, because they rely on the use of two keys: a public key and a private key. Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named, you guessed it, for its inventors), and DSA, the Digital Signature Algorithm, (invented by David Kravitz).
There are many ways an investigator might try to break encrypted data. If they have access to the encryption software, they could study how the algorithm worked, identify any weaknesses, and try to work out how to break it. Even if the algorithm is hard to break, the software may be poorly designed. Some software accidentally copies the unencrypted message onto the hard disk. Also, some algorithms have known weaknesses and tools are available to break them.
The proposed work will help to strengthen data security and develop an algorithm which will be hard for breaking encryption [3].

Objective:-

- Database security solutions for the home and enterprise.
- To develop an effective standardized disclosure system.
- To help users to mitigate or eliminate them.

## II. Review of previous research in the area and justification

In Conventional Cryptography both users use the same key to encrypt and decrypt messages to provide confidentiality, but they cannot provide authentication or no repudiation. There is no way to prove who actually sent a message if two people are using the exact same key where as on Public-Key Cryptosystems Works much slower than conventional cryptography.

Volume: 03 Issue: 05 Pages:29-35 (2012)
*Special Issue of NCETCSIT 2011 - Held on 16-17 Dec, 2011 in Bapurao Deshmukh College of Engineering, Sevagram*

The proposed work aims to keep the strength of previous work but discard there weakness to strengthen data security against is attackers. [4]

Plaintext is converted into cipher text by means of an encryption engine whose operation is fixed and determine (the encryption method), but which function in practice in a way dependent on a piece of information (the encryption key) which has a major effect on the output of the encryption process [5].

## III. Literature review

Brief History of Cryptography

Cryptography is combined with methods of ensuring the secrecy and authenticity of message. A cryptographic algorithm, also called cipher, is a mathematical function used for encryption. In most cases, two related functions are employed, one for encryption & other for decryption. Encryption is the process of transforming information so that it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again to the intended recipient. An eavesdropper who intercepted the transmitted message receives only "garbage" (the cipher text), which makes no sense to him since he does not know how to decrypt it [6].

When someone wants to access to the computer system there must be some way that he can convince it of its identity. Once it knows your identity, it can verify whether you are entitled to enter the system. The same principal applies when one person tries to communicate with another as a first step you want to verify that you are communicating with the right person. Therefore there must be some way in which you can prove your identity. This process is called user authentication. There are several ways to obtain user authentication. You can give him something only you can know like a password, user-id, a pin code, and so on. Or you could have some specific items with which you can identify yourself like a magnetic strip card, a smart card. One might make use of biometric properties; it is a well-known fact that fingerprints, the shape of the hand and retinal pattern of a person are good decision criteria. These however require specialized equipment and thus a big investment. Other techniques include measurements of how a person types his name or writes his signature, or can take into account the location of the user [7].

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing [8].

2000 years ago, the Greek knew cylinder device called Scytale, which was the sender's part very similar to the recipient part, where a narrow strip of parchment or leather, was wounded around the Scytale and the message was written across it, so if anyone tries to read the text he will find meaningless letters, The only one that can read this text is the one who has the Scytale, This technique is similar to the transposition technique [9].

A method of encryption and decryption is called a cipher. Some cryptographic methods rely on the secrecy of the algorithms; such algorithms are only of historical interest and are not adequate for real-world needs [10].

Symmetric (Secret or Conventional Key) Cryptography

In this type of cryptosystem, there is only one key shared by both sender and receiver. If the sender wants to send some secure information, first he has to generate one key and then encrypt the information using same key, so after he has to send that key via some secure channel to the receiver, the receiver can decrypt the cipher text by using the same key which was sent to him by sender and that is how receiver can retrieve real information that was intended for him.

Example of Symmetric Cryptography Algorithm

- DES – Data Encryption Standard
- 3DES – Triple DES
- AES – Advance Encryption Standard
- Blowfish
- RC5, RC6, etc.

*DES* (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) . Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [11],[12].

*3DES* is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [11].

Triple DES is a minor variation of this standard. It is three times slower than regular DES but can be billions of times more secure if used properly. Triple DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. In 1998 the Electronic Frontier Foundation, using a specially developed computer called the DES Cracker managed to break DES in less than 3 days. The encryption chip that powered the DES Cracker was capable of processing 88 billion keys per second. Any organization with moderate resources can break through DES with very little effort these days.

*AES* is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms

Volume: 03 Issue: 05 Pages:29-35 (2012)
*Special Issue of NCETCSIT 2011 - Held on 16-17 Dec, 2011 in Bapurao Deshmukh College of Engineering, Sevagram*

especially in small devices. Also, AES has been carefully tested for many security applications [13].

*Blowfish* is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less [14].

RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard [15].

We also examine a method for evaluating performance of selected symmetric encryption of various algorithms. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies.
This causes a "battery gap" [16], [17].We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices.

Asymmetric (Public Key) Cryptography

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called "private key" or "secret key", while the encryption key is spread to all who might want to send encrypted messages, therefore called "public key". Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie Hellman [18].

Examples of Asymmetric Cryptography Algorithm

- RSA - Rivest-Shamir-Adleman
- DSA – Digital Signature Algorithm
- ECC – Elliptic Curve Cryptography

Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) was proposed by Victor Miller and Neal Koblitz in the mid 1980s. The main advantage of elliptic curve cryptography is that the keys can be much smaller. Recommended key sizes are in the order of 160 bits rather than 1024 bits for RSA [19].

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and released in 1991. It was the first widespread public key encryption program. PGP is a complete working system that uses cryptographic protection to protect e-mail and files. It mainly uses RSA public key encryption for key management and IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms to use. PGP can provide confidentiality through the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation through the use of cryptographically signed messages.

PGP is a one type of program that provides Privacy to your electronic mail. What it does is simply encrypt your e-mail so that nobody in the world but the intended recipient person is able to read it. Another use of the PGP is to sign the document digitally without encrypting it. For instances, in public postings where if you don't want to hide yourself and what you are saying, but rather want to allow others to confirm that the message actually came from you. The good thing of digital signature is that once a digital signature is created. It is impossible for anyone to modify either the message or the signature without the modification being detected by PGP. So there is no possibility of forgery [20].

S/MIME (Secure Multipurpose Internet Mail Extension )

Secure MIME (S/MIME) is a standard for encrypting and digitally signing electronic mail that contains attachments and providing secure data transmissions. S/MIME extends the MIME standard by allowing for the encryption of e-mail and attachments. The encryption and hashing algorithms can be specified by the user of the mail package instead of having it dictated to them.
S/MIME provides confidentiality through the user's encryption algorithm, integrity through the user's hashing algorithm, authentication through the use of X.509 public key certificates, and nonrepudiation through cryptographically signed messages.

S/MIME is an extension of the popular MIME (Multipurpose Internet Mail Extension) electronic mail standard that adds security to protect against interception and e-mail forgery. The demand for e-mail security is growing along with a demand to validate the authenticity of messages [21]. It is too easy for someone to post a message in a public forum that appears to be from someone else. E-mail security lets users electronically sign messages to prove their origin. Basically, S/MIME is designed to secure messages from prying eyes.

Digital Signature

Some public-key algorithms can be used to generate digital signatures. A digital signature is a block of data that was created using some secret key, and there is a public key that can be used to verify that the signature was really generated using the corresponding private key. The algorithm used to generate the signature must be such that without knowing the secret key it is not possible to create a signature that would verify as valid .

Volume: 03 Issue: 05 Pages:29-35 (2012)
*Special Issue of NCETCSIT 2011 - Held on 16-17 Dec, 2011 in Bapurao Deshmukh College of Engineering, Sevagram*

WITH the rapid development of the Internet and the rise of E-business and E-commerce, data confidentiality, authenticity, integrity, and non-repudiation are basic concerns regarding data exchanged over an open network. A digital signature (DS) can provide the function of a conventional handwritten signature for the goals of entity authentication, data integrity, and non-repudiation [22]. DS is an important method in public-key (asymmetric) cryptography. In 1976, Diffie and Hellman [8] first introduced the concept of digital signature, which is a verification scheme that concentrates on data authenticity [9], [10]. Most current digital signature schemes are based on mathematical algorithms that require very complex mathematical computations. Therefore, the sender (signer) has to depend on a computer to digitally sign a document. Also, the receiver (verifier) has to use a computer to check the validity of the signature [23]. Until now, building a digital signature scheme with high security and without complex mathematical computations has been a great challenge.

Hash Function

A hash function is an algorithm to create a digital representation or fingerprint in the form of the hash value is the standard length. The hash function is usually much smaller than the message, but unique. Any change in the message invariably produces a different hash result when the same hash function is used. It is computationally infeasible to derive the original message from knowledge of the hash value. This mode is called one- way hash function or dynamically hashes function, just suitable for one time and change the hash function time to time. The hashing function is applied on the message; where there are 4 tables of the hashing character are used by replaced it by the original character (character of reading message). These tables contain all characters available in the keyboard; with the additions English and Arabic characters. Total characters in this table are 133 characters.

Hash functions are required to satisfy a variety of different security requirements in cryptographic schemes. In fact, in the past, hash functions were viewed by practitioners as black-boxes with magic properties.

However, this perception has changed since the recent attacks on existing hash functions, including the SHA-1 and MD5. Most notable of these were the new and improved collision-_finding attacks proposed by Wang et al [24]. Along with other results demonstrating weaknesses of existing hash function constructions, such as [24, 25], these attacks showed that the collision-resistance of these hash functions is much worse than what was anticipated earlier. Moreover, these results have also cast a doubt on the security of these hash functions with respect to other notions.

Statement of the problem:-

The problems include:

A. Authentication (to prevent unauthorized users).
B. Encryption (to prevent users not in the identify setup information).
C. Privacy and Confidentiality
D. To maintain data security of system

Scope:-

1. Electronic information security at home, and also within organizations needs to secure their data security hence can implement proposed work which is easy-to-use, easy-to-administer, cost efficient and more secure.
2. The proposed work will develop such a system that support secure, location independent information sharing.
3. The system will allow flawless and secure sharing of information.
4. Secure enterprise applications by discovering, assessing and protecting the database against rapidly changing security threats.
5. It is not easy for hackers to break

## IV. Proposed methods

Hybridizing traditional method of Cryptography which includes symmetric and asymmetric, a new way of encrypting data will emerge which is more reliable and user friendly and difficult for breaking encryption This method of Hybridizing data will be called Hybridizing Traditional Technology (H.T.T) algorithm, which involves following steps:

- Collection of Plaintext i.e. data.
- Converting it into cipher text using H.T.T encryption algorithm.
- Cipher text can be converted back into Plaint text using H.T.T decryption algorithm.

The Strength of Encryption

The strength of encryption is important in accordance with the required time to decode a key.

The calculation of encryption strength of an encryption algorithm is calculated below.

$\underline{((\text{Differential Characteristic})^{-1}/2))} * \text{Computer Speed}$ (1)

second (1h) * 24 h * 365 days

Because of the plain text divided into 128 blocks of $2^8$ bits the Probability Filtered pairs chosen as $2^8$

Probability Filtered Pairs $(P1xP2)^{-1} = (2^8 x 2^{8)-1} = 2^{-16}$ (2)

Differential Characteristic (DC) — Probability Filtered Pairs x Filtered weight (3)

$=2^{-16} x2^{-8}$

$= 2^{-24}$ (4)

For proposed algorithm DC equal $2^{-96}$ because in this algorithm there are four rounds.

Then now we can compute the time needed to crack this algorithm

$(2^{96}/2)x883 x10^6/ 3600 x24.x365= 1.11E+30year.$ (5)

Volume: 03 Issue: 05 Pages:29-35 (2012)
*Special Issue of NCETCSIT 2011 - Held on 16-17 Dec, 2011 in Bapurao Deshmukh College of Engineering, Sevagram*

## V. Result

The result which get in the experimental process are coming from the calculating of time consuming in both operations "encryption, decryption" and compare it with RSA algorithm, the evaluation of the strength of the proposed algorithm was calculated in this processes.
This comparison was conducted on three text files sized of 200 kb, 350 kb and 500 kb for both algorithms. For the proposed algorithm as shown in the table 1.1, table 1.2, and table 1.3 where use four encrypted data tables which names (tb1, tb2, tb3, and tb4) stored in the main software program. For each of the encrypted table the encryption and decryption time were calculated.

Table 1.1: encryption /decryption time using proposed algorithm for file size 200kb

| Table # | The | Tdr | size |
|---|---|---|---|
| Tbl | 9.2lms | 12.2Sms | 200kb |
| Tb2 | 1 0.23ms | 13. l4ms | |
| Tb3 | 9.54ms | l1.42ms | |
| Tb4 | 9.88ms | l1.74ms | |
| | Avg 9.71 ms | Avg12. l4ms | |

The: Time to compute hashing and encryption
Tdr: Time to compute decryption and rehashing

Table 1.2: encryption and decryption time using proposed algorithm for file size 350kb

| Table # | The | Tdr | Size |
|---|---|---|---|
| Tbl | 12.4lms | 15.23ms | 300kb |
| Tb2 | 1l.44ms | 14.95ms | |
| Tb3 | 11.85ms | 15.04ms | |
| Tb4 | 11.32ms | l4.88ms | |
| | Avg11.76ms | Avg15.02ms | |

The: Time to compute hashing and encryption
Tdr: Time to compute decryption and rehashing

Table 1.3: encryption and decryption time using proposed algorithm for file size 500kb

| Table # | The | Tdr | Size |
|---|---|---|---|
| Tbl | 18.12ms | 21.02ms | 500kb |
| Tb2 | 16.52ms | 19.55ms | |
| Tb3 | 16.58ms | 19.88ms | |
| Tb4 | 17.02ms | l9.02ms | |
| | Avg11.76ms | Avg15.02ms | |

The: Time to compute hashing and encryption
Tdr: Time to compute decryption and rehashing

The average time of all encrypted tables calculated as well For RSA algorithm.
Encryption and decryption time were calculated as shown in Table 1.4.

Table 1.4: Encryption and Decryption Time Using RSA Algorithm

| Size | Te | Td |
|---|---|---|
| 200kb | 32.56ms | 57.62ms |
| 350kb | 67.96ms | 112.2 3ms |
| 500kb | 102.23 ms | 182.56ms |

Discussion:-
Multiple comparisons were done on the previous results. The first comparison is given between the encryption and decryption time of text file with size 200Kb, in the second and third same comparison but with the 350Kb, 500Kb respectively. The last one calculates the time of same text files with the RSA algorithm.
Fig 1.1 shows the comparison time for encryption of both algorithms, here we found RSA algorithm consuming a long time to complete the encryption operation for all files compared with the proposed algorithm. And the file with size 500Kb take the longest time 102.23ms then 350Kb and finally 200Kb.

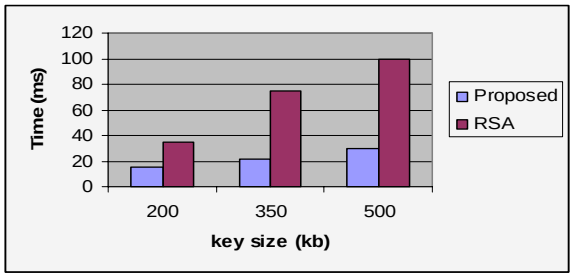


Figure 1.1 : Encryption Time in Both Algorithms

Fig 1.2 shows the comparison time for decryption of both algorithms, here we found RSA algorithm consuming a long time to complete the decryption operation for all files compared with the proposed algorithm. And the file with size 500Kb take the longest time with value 182.56ms then 350Kb and finally 200Kb.

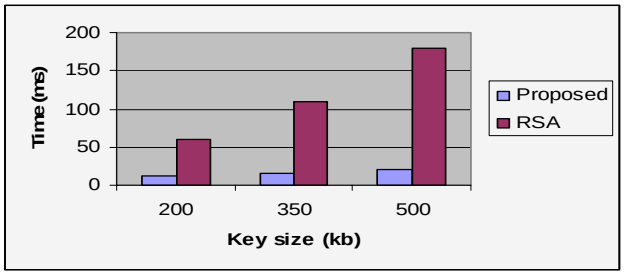


Figure 1.2 : Decryption Time in Both Algorithms

As shown in Table 1.5, the stability of the proposed algorithm is higher than SEED, DES and RSA Algorithm.

Table 1.5: Comparison of encryption Strength

| Index | Algorithm Name | Key Size | Needed Time (year) |
|---|---|---|---|
| 1 | SEED | 1024 | 2.7 E +21 |
| 2 | DES | 1024 | 2.5E+9 |
| 3 | RSA | 1024 | 7.3E+26 |
| 4 | PRPPOSED ALGORITHM | 1024 | 1.11E+30 |

The fig 1.3 shows the comparison of needed time (years) to crack some of algorithms, where we found that proposed algorithm has a highest strength, and need a long time to crack than SEED, DES, and RSA algorithms respectively. The purposed algorithm as we can show from the table needs 1.11 E+30 year.

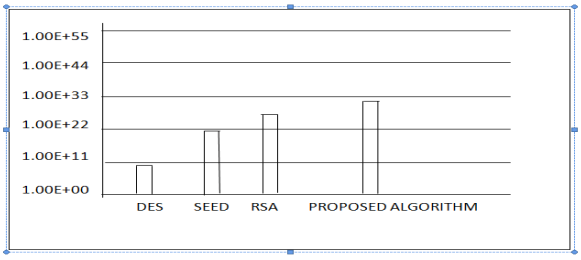


Figure 1.3: Cracking Time in Different Cryptography Algorithms

## VI. Conclusion :-

A modified data encryption standard algorithm for data security has been proposed in this paper. The proposed algorithm (HTT) was developed based on the combination of symmetric and asymmetric algorithm whereas the length of the key and digital signature was considered. In this manner, the length of the key would not affect the time execution of this algorithm and digital signature in the end of message would increase the authentication between the sender and the recipient.

The implemented algorithm has been used to encrypt and decrypt a different size of text file and compare the results with one of the most popular and used cryptographic algorithms (RSA). From the results, it can be noticed that the execution time of the proposed algorithm was less than the compared algorithm (RSA) and has given a better time in encryption and decryption operations.

Based on the computing of strength algorithm it can be observe the time of cracking of this algorithm is long than the AES ,DES, and RSA algorithms on the same, where the hacker need a 1.1 E +30 years to crack this algorithm.

REFERENCES :-

[1] Salomao, S. L. and., Alcantara, J. M., Alves, V. C., Franca, F. M. (2000). *Improved IDEA Integrated Circuits and Systems Design, Vol*. 9.pp. 47 — 52.

[2] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley.*

[3] John, J. G. (2004). *International Data Encryption Algorithm*,. [online] http://www.andrew. cmu.edu/user/lmai/525/four. html (Accessed on 12 Mar 2005).

[4] Mayer, P. (1994). *Introduction to Cryptography*, [online] http://www.totse.com/en/privacy/encryption/165727.html. (Accessed on 12 Apr 2005).

[5] AL- Salqan, Y. Y. (1997). *Distributed Computing System. 6th IEEE Workshop on Future Trends of Distributed Computing Systems*, PP. 34- 37.

[6] Rabah, K. (2004). Data Security and Cryptographic Techniques—*A Review, Asian Network for Scientific information.Technology Journal 3, Vol. 1*. pp. 106-132.

[7] Bide, M. and Hing, T. (1998). *User Identification and Authentication:*
A brief Introduction. Book industry Communication and EDITEUR.

[8] J.R Childs: " General Solution of the ADFGVX Cipher System ". Aegean Park Press, ,(2000), USA.

[9] G .Dieter: " Computer Security ", Second Edition. John Wiley & Sons, ,(2005), UK.

[10] Groenewegen, S. and Buchner, A. (1999). *The Basics of Cryptography*,. [online] http://www.nuitari.de/crppto.html.(Accessed on 14 Feb 2005).

[11] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[12] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."*IBM Journal of Research and Development*, May 1994,pp. 243 - 250.

[13] Daemen, J., and Rijmen, V. "Rijndael: *The Advanced Encryption Standard."D r. Dobb's Journal*, March 2001,PP. 137-139.

[14] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/blowfish.html
[15] N. El-Fishawy ,"Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, , Nov. 2007, PP.241–251
[16] K. McKay, "Trade-offs Between Energy and Security in Wireless Networks Thesis," Worcester Polytechnic Institute, April 2005.
[17] R. Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9 , Issue 2 ,May. 2006.
[18] Hart, L. (1999). *Securing Messaging Middleware Applications, Business integration, Optimizing Business integration & Effectiveness*Through Leading- Edge Technologies. Academic Press.
[19] Engelfriet, A. (2005). *Elliptic curve cryptography*, [online] http://www.iusmentis.com/technology/encryption/elliptic-curves. (Accessed on 18 Mar2005).
[20] Patel, V. Chandra, A. Jain, S. (2001). *Electronics mail security Pretty Good Privacy (PGP) & Secure Multipurpose Internet Mail Extensions (S/MIME),* MS.C Thesis George Mason University.
[21] Argyroudis, P. G. Verma Tewari, H. O'Mahony, D. (2004). Perfirmance Analysis of Crvptographic Protocols on Handheld Devices, *IEEE International Symposium on Network Computing and Applications,* pp. 169-174.
[22] F. Yang, "Cryptanalysis on an Algorithm for Efficient Digital Signatures," Cryptology ePrint Archive 2005/456, 2005.
[23] W. Stallings, *Cryptography and Network Security-Principles and Practices*, Prentice Hall, Inc, 4th Ed., 2006.
[24] J. Kelsey and T. Kohno, Herding Hash Functions and the Nostradamus Attack, Advances in Cryptology - EUROCRYPT 2006, 183-200.
[25] X. Wang, H. Yu, Y. L. Yin, Efficient Collision Search Attacks on SHA-Advances in Cryptology - CRYPTO 2005, 1-36.

**Biographies and Photographs**

**Photograph and Author's Profile:**
**Swapnil Govindrao Deshpande,** Lecturer, Vinayak Vidyamandir, Amravati (MH)

**Author's profile;**
**Swapnil G. Deshpande** is working as Lecturer in Computer Science at Amravati. He has 5+ years of teaching experience. He teaches Networking, System Analysis and Design, DBMS, OOP in B.C.A. and MCM program. He was born on August 10, 1983 in Amravati, Maharashtra, India.
**Swapnil G. Deshpande** got B.Sc Degree from Amravati university in 2004 and he done his post graduate degree from Amravati Univeristy in 2006 and M.phil from Yashwantrao Chavan Open Univeristy in 2009. Since 2006 till now he is working as a computer lecturer in Amravati Univeristy, Maharashtra, India. His research interest includes Mobile Computing, Image Processing, Data Mining, Computer Networks, Cryptography, Image Processing, Multimedia applications, data hiding Network Security and Soft Computing Techniques. He has 1 research paper publications in National Conference. He has explored the subject of network security and cryptography to a large extent in his M.Phil thesis, he is working on the new concepts to avoid sending the key over and over again and make the best use of both symmetric and asymmetric key algorithms.
**********

**Dr**.**Pradeep B. Dahikar,** Associate Professor.[ Head ], Kamla Nehru Mahavidyalaya, Nagpur-9.

**Author's profile;**
**Dr**.**Pradeep B. Dahikar** is working as Associate Professor.[ Head ], Kamla Nehru Mahavidyalaya, Nagpur-9
He has U.G. 19Years , P.G. 15 Years of teaching experience.
He was born on 20$^{th}$Jun 1963. He got B.Sc Degree from Amravati university in 1988 and he done his post graduate degree from Gour Univeristy Sagar in 2008. His research interest includes Thermoluminescence Materials & Development of Related low coast Instruments. He has published 6 International and 45 National Journals. He obtained his Ph.D. degree in Electronics from University of Nagpur, India in 2008. He has total 09 years Research Experience and he attended 29 Conferences/Seminar/Work Shops. ***Total 10 Research student registered for Ph.D Program and 8*** M Phil Student completed their project/ Dissertation.
**********