

A Survey on Network Security and Security Authentication using Biometrics

Chirag Singh Sisodia¹ Aparajit Shrivastava²

^{1,2}Department of Computer Science
^{1,2}SRCEM, Morena, India

Abstract—To create secure information transmission over the network cryptography is used. The algorithm particular for cryptography should complete the integrity protection condition, conventional information authentication and digital signatures. Key exchange algorithms, hash functions, PN numbers are used for encryption and decryption of data.. Here in our paper, we are studying present algorithms currently used for encryption. Cryptography has been emerged as an essential tool for data transmission. There are various techniques of cryptography, both asymmetric and symmetric. The review is complete on few of the additional common and also interesting algorithms of cryptography presently in use and their drawbacks and also benefits are also discussed. In this paper, it has been surveyed about current works on encryption techniques. Those methods of encryption are studied and also analyzed well to performance promote of the encryption approaches also to guarantee the security proceedings. This paper presents the performance evaluation of algorithms of the selected symmetric. The particular algorithms are AES, 3DES, Blowfish and also DES.

Key words: Cryptography, AES, Blowfish, 3DES, Biometrics

I. INTRODUCTION

Cryptography [1] is a secret writing science. It is the information protecting art through transforming it into an illegible format in which a information can be concealed from the reader and also intended recipient will be able to the convert it into original data. Its basic goal is to security of the information from unauthorized access. [1] Information can be read and also understood without any particular measures is known as plaintext. The disguising plaintext technique in such a way as to the hide its substances is known as encryption. Encrypting plaintext outcomes in unreadable gibberish known as ciphertext. The reverting procedure of cipher text to its original plaintext is known as decryption. A system gives decryption and encryption is called cryptosystems. Cryptography gives number of security objectives to guarantee the protection of information, on-change of information et cetera. Because of the colossal security points of interest of cryptography it is broadly utilized today. Taking after are the different objectives of cryptography.

A. Confidentiality

Computer data is transmitted and has to be retrieved only through the official party and not with anyone else.

B. Authentication

The data received through any system has to identity check of the sender that whether information is arriving from a authorized access or the false identity.

C. Data Integrity

Confirming the data has not been changed through unauthorized or unidentified that means no one in between the receiver and sender are permitted to alter the provide information.

D. Non Repudiation

Prevents either receiver or sender from denying a data. Thus, when a information is sent, receiver can be prove that the information was in fact send through the alleged sender. Similarly, when a information is received, the sender can prove the alleged receiver in fact received the information.

E. Access Control

Only the authorized parties are able to access the provide data.

II. DEFINITION & TERMINOLOGY

Cryptography describes art and science of the transforming information into a bits sequence that shows up as arbitrary furthermore insignificant to a side attacker or observer.

Cryptanalysis [2] is the reverse cryptography engineering—challenges to classify weaknesses of numerous algorithms of cryptographic and their implementations to exploit them. Any attempt at cryptanalysis is well-defined as an attack.

Cryptology encompasses both cryptanalysis and also cryptography and looks at mathematical issue that underlies them.

Cryptosystems are computer systems used to the encrypt information for secure transmission and also storage.

Plaintext is a message or information which are in their normal, readable (not crypted) form.

Encryption: Encoding the information contents in such a way that hides its contents from outsiders.

Cipher text outcomes from plaintext through using the encryption key.

Decryption: The retrieving procedure the plaintext back from the cipher text.

Key: Decryption and Encryption commonly create use of a key, and the coding technique is such that decryption can be achieved only through knowing the proper key.

Steganography is the hiding secret data technique in an ordinary document. Steganalysis could be easily described as the steganography detection through a third party. Hash functions create an information digest. Substitution cipher includes an alphabet replacing with another different character of the same alphabet set. Mono-alphabetic system uses a single alphabetic set for substitutions. The Poly-alphabetic system uses multiple of alphabetic collection for substitutions. Caesar cipher is a mono-alphabetic method in which all characters are changed

through the third character in succession. Julius Caesar used this encryption method.

A computerized mark is a data block that is created through the sender of a information applying his/her secret key.

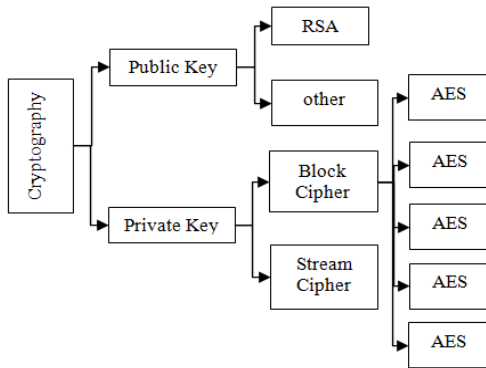


Fig. 1: commonly used encryption technique

III. CLASSIFICATION OF CRYPTOGRAPHY

Cryptography can be divided into two major category based on the use of key.

A. Symmetric Encryption (Private Key Encryption):

In this sort of encryption same key is utilized at the encryption and decoding time. The key dispersion must be made before the data's transmission begins. The key assumes a critical part in this kind of encryption. Example: DES, 3DES, BLOWFISH, AES etc.

B. Asymmetric Encryption (Public Key Encryption):

In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts. [3] Example: RSA algorithm.

IV. ENCRYPTION ALGORITHM

This subsection characterizes furthermore looks at prior chip away at most well known algorithm.

A. DES

Data encryption standard is a block cipher that uses shared secret key for decryption and encryption. Data encryption standard estimation as described through Davis R. [3] takes a plaintext bits fixed-length string and also transforms it by a complicated operations series into same length cipher text bit string.

In the DES case, all size of square is 64 bits. Data encryption standard also uses a 56 bits key to the transformation customize, so that decryption can only be achieved through those who know the specific key used to message encrypt. There are 16 identical processing stages, termed rounds. There is also permutation of an initial and also final, termed FP and IP, which are inverses (IP "undoes" the action of FP, and vice versa). The Broad level phases in data encryption standard are as follows [1]:

- 1) In the first level, 64-bit plain text information is handed over to an IP (Initial permutation) function.
- 2) The IP is achieved on plain text.

- 3) The Initial permutation creates two different halves of the permuted information; LPT (Left Plain Text) and RPT (Right Plain Text).
- 4) Now, all of RPT and LPT go by 16 rounds of encryption procedure.
- 5) In the end, RPT and LPT are rejoined and a FP (final permutation) is performed on the combined block.
- 6) The outcome of this procedure produces 64-bit cipher text.

Rounds: all of the 16 rounds, in turn, consists of the broad level steps and present in Figure.

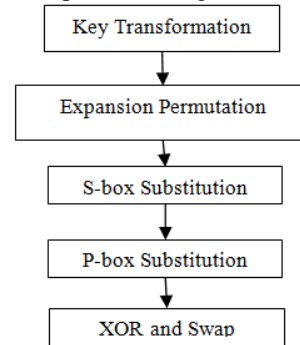


Fig. 2: Details of One Round in DES

B. 3DES

3DES (Triple DES) is an improvement of DES; it is a 64 bit piece size through 192 bits key size. In this standard the strategy for encryption is same to the one in the first DES yet connected 3 times to development the encryption level furthermore the normal safe time. 3DES is slower than other distinctive piece figure approaches. It utilizes either a few diverse 56 bit keys in the succession EDE (Encrypt-Decrypt-Encrypt). Essentially, three different keys are utilized for the encryption calculation to make figure content on plain instant message, t.

$$C(t) = Ek_1(Dk_2(Ek_3(t))) \quad (1)$$

Where C(t) is cipher text produced from plain text t,

Ek1 is the encryption method using key k1

Dk2 is the decryption method using key k2

Ek3 is the encryption method using key k3

Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$$C(t) = Ek_1(Dk_2(Ek_3(t))) \quad (2)$$

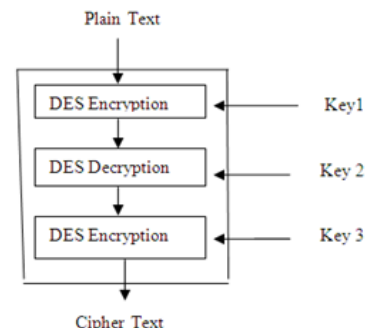


Fig. 3: Encryption in 3DES

Algorithm of TDES with the three different keys need 2^{168} probable combinations and also two different keys need 2^{112} combinations. It is essentially not possible to try such a large combination so TDES is a algorithm of

strongest encryption. The algorithm drawback it is too time consuming.

C. AES

The AES cipher [6] is practically identical to the block cipher Rijndael cipher developed with two different Belgian cryptographers, J. Daemen and V. Rijmen. The algorithm defined through AES is a symmetric-key algorithm, significance the same key is used for both data encrypting and decrypting. The internal rounds number of the cipher is a function of the key length. The various rounds for 128-bit key is 10. Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an complete block per iteration, e.g., in DES, $64/2 = 32$ bits are encrypted in one round. AES, on the other different hand, scrambles every one of the 128 bits in one cycle. This is one motivation behind why it has a similarly little number of rounds.

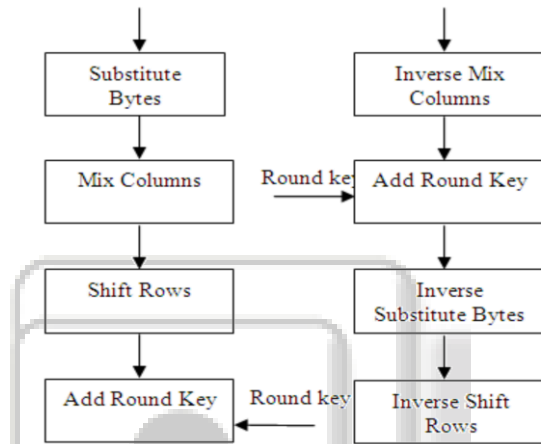


Fig. 4: One Round of Decryption and encryption in AES
Encryption Round Decryption Round all processing round contain four different level:

- Substitute byte: a non-linear substitution level where all byte is changed with another according to table of a lookup.
- Shift rows: a transposition level where every state row is shifted cyclically a various level.
- Mix column: a mixing operation which operates on the state columns, combining the four various bytes in every column.
- Add round key: every state byte is combined with the round key applying bitwise XOR.

AES encryption is flexible and fast. It can be implemented on numerous platforms particularly in small devices.

1) AES Encryption:

The encryption procedure in the AES contains following level:

- a) Do the one-time initialization procedure:
 - Expand 16-byte key to found the actual Key Block to be used.
 - Do one time initialization of the 16-byte plain text block (called State).
 - XOR the state with the key block
- b) For all rounds do the following:
 - Using S-Box to all of the plain text bytes.
 - Rotate row k of the plain text block (i.e. state) by k bytes.

- Perform mix columns process.
- XOR the state with the key block.

D. Blowfish

Blowfish [5] is one of the most famous public domain encryption algorithms providing through Bruce Schneier – one of the world's leading cryptologists, and the Counterpane Systems president, a accessing firm specializing in cryptography and also security of the computer. The Blowfish algorithm was first presented in 1993. The blowfish encryption is present in figure below:

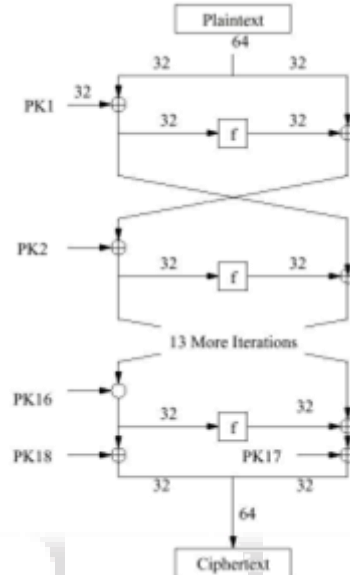


Fig. 5: Blowfish Encryption

1) Operation of Blowfish:

Blowfish encrypts 64-bit block cipher with a variable length key. It include two different parts

- a) Subkey Generation: This procedure changes the key up to 448 bits long to subkeys to totaling 4168 bits.
- b) Data Encryption: This procedure contains the iteration of a simple function 16 times. All round include a key ward stage and key-and information subordinate substitution.

Blowfish suits the applications where the key stays consistent for a drawn out stretch of time (e.g. Correspondence join encryption) however not where the key changes regularly (e.g. parcel exchanging).

E. RSA

RSA is a public key algorithm designed through Rivest, Shamir and Adleman [7]. The key utilized for encryption is unique from the key utilized for unscrambling. RSA contain private key and an public key. People in general key can be known not and is utilized for encoding messages. Messages scrambled with the general population key must be decoded with applying the private key. The keys for the RSA algorithm are made the accompanying way:

- Selected two different distinct large prime numbers p and q.
- For security purposes, the integer's p and q should be chosen at random, and should be of similar bit length. Prime integers can be efficiently found with applying a primarily test.

- Compute $n = pq$; n is used as the modulus for both the public and private keys
- Select the public key (i.e. the encryption key) E such that it is not a factor of $(p - 1)$ and $(q - 1)$.
- Select the private key (i.e. the decryption key) D such that the following equation is true:
$$(D * E) \bmod (p-1)(q-1) = 1$$
- For encryption, calculate the cipher text CT from the plain text PT as follows:
$$CT = PT^E \bmod N \quad (3.1)$$
- Select CT as the cipher text to the receiver.
- For decryption, calculate the plain text PT from the cipher text CT as follows:
$$PT = CT^D \bmod N \quad (3.2)$$

V. ADVANTAGES AND DISADVANTAGES OF ENCRYPTION ALGORITHM

A. DES:

Advantages and Disadvantages of the data encryption standard are

1) Advantages

- The data encryption standard algorithm has been a most common secret key algorithm of encryption and is used in the numerous commercial and also financial applications.
- Although presented in the 1976, it has proved resistant to each cryptanalysis forms.

2) Disadvantages

- Its key size is too much less through present and its whole 56 bit key space can be looked in roughly 22 hours.2) It was recognized that data encryption was not secure because of advancement in computer processing power

B. 3DES:

1) Advantages

- It uses 64 bit block size with the 192 bits of key size. It is simple like DES because the encryption technique is similar to the one in the original data encryption standard but applied 3 times to growth the encryption level and the average safe time.
- 3DES are simply to the implement (and accelerate) in both software and hardware.

2) Disadvantages

- 3DES is slower than other different method of block cipher.
- It has poor performance.

C. AES:

1) Advantages

- The main purpose of the advance encryption standard algorithm is to replace the older and also less reliable algorithms, such as DES (Data Encryption Standard).
- Advance encryption standard is fast and flexible encryption method.
- The advance encryption standard has also been employed in other different areas such as to secure data in smart cards and also online transactions.
- Until May 2009, the only effective distributed attack against the full propel encryption standard were side-channel assaults on some particular executions.

- In June 2003, the U.S. Government declared that AES could be utilized to secure classified data.
- The outline and quality of every key length of the AES calculation (i.e., 128, 192 and 256) are adequate to ensure arranged information up to the SECRET level. TOP SECRET information will oblige utilization of either the 192 or 256 key lengths.

2) Disadvantages

- Advance encryption standard in the GCM (Galois/Counter Mode) is most challenging to the implement in software.
- The key length size is too long that creates it complex sometimes.

D. Blowfish:

- Blowfish is block cipher 64-bit, which can also be used as a DES algorithm replacement. It takes a variable length key, ranging from the 32 bits to 448 bits; default 128 bits.
- Blowfish is fast as its encryption rate of 32-bit microprocessor is 26 clock cycles per byte.
- It is compact as it can perform in the less than 5 KB memory.
- It is easier because it usages only primitive operations for example addition, XOR and table lookup, creating its design and also implementation simple.
- It has a variable key length upto a maximum of 448 bits long making it both flexible and also secure.
- No attack is known to be successful against this. Blowfish is unpatented, license-free, and is presentable free for each uses. Blowfish has variants of 14 rounds or less.
- Blowfish is considered to be the best out of all encryption algorithms.

E. RSA:

1) Advantages

- The primary RSA advantage is increased security: as the private keys do not ever need to be transmitted or revealed to anyone. Whereas in a secret-key system, there is always a chance that an enemy could discover the secret key while it is being transmitted.
- Another major public-key systems advantage is that they can give a digital signatures technique. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well.
- Digitally signed information can be proved authentic to a third party, such as a judge, thus permitting such information to be legally binding.

2) Disadvantages

- A disadvantage of applying public-key cryptography for purpose of encryption is speed: they processing are very slow.[4]

VI. LITERATURE SURVEY

Mitali (2014) t al present that In the current era, networking evaluation and also wireless networks has come forward to grant communication anywhere at any time. wireless networks Security is nasic aspect and the cryptography procedure perform most significant role to security provide

to the wireless networks. There are numerous techniques of cryptography both asymmetric and symmetric. The survey is complete on some of the more common and also interesting cryptography algorithms presently in use and their disadvantages and advantages are also discussed. This paper gives a fair performance comparison between the numerous cryptography algorithms on various data packets settings. In this paper, we analyze the decryption and encryption time of numerous algorithms on various data settings. In this wireless world currently, the data security has become extremely significant since the selling and also products buying over the open network happen very frequently. In this paper, it has been surveyed about the current works on the encryption methods. Those encryption methods are considered and investigated well to advance the encryption's execution strategies likewise to guarantee the security procedures. This paper displays the chose symmetric calculations execution assessment. The chose calculations are AES, 3DES, Blowfish and DES.[4]

Pranab Garg (2012) et al present that To make secure information transmission over systems cryptography is utilized. The calculation chose for cryptography ought to satisfy the states of uprightness assurance, customary message verification and computerized marks. Key trade calculations, hash capacities, PN numbers are utilized for encryption and unscrambling of information. This encryption can be connected on information in stream group or in squares. In addition the length of key is the greatest limitation in encryption. Here in our paper we have examined present calculations as of now utilized for encryption.

Cryptography has been emerged as essential tool for data transmission. Various algorithms of cryptography has been studied, If advantages of all these algorithms are combined in one algorithm then performance of cryptography can be increased along with the length of key. In public key algorithm for generation of private key CDMA approach of communication can be used. Each user is provided a Different unique number called PN number and no other user is having that number. For each user this unique number is generated randomly and at the receiver end same PN number can be used to decrypt the message.[5]

Shivangi Goyal (2012) et al present that This paper gives a brief rundown of cryptography, where it is connected and its utilization in different structures. Cryptography is a method for defending the critical information from unapproved access. It has risen as a protected means for transmission of data. It chiefly helps in controlling interruption from outsider. It gives information classification, honesty, electronic marks, and propelled client confirmation. The systems for cryptography use arithmetic for securing the information (encryption and

unscrambling). In this exploration paper the pertinence of cryptography in information security has been contemplated and outlined. Additionally the different cryptographic strategies have been watched and their particular regions of appropriateness have been figured out and a condensed table has been developed.[6]

A. Joseph Raphael Digital communication has become an important infrastructure part currently, a various applications are Internet-based and it is significant that communication be made secret. As a outcome, the information security passed over an open channel has become a fundamental subject and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has occasioned in an information hiding unbalanced development. Steganography and Cryptography are the two different famous approaches presentable to provide security. One hides the message existence and the other different distorts the message itself. Applying cryptography, the information is transformed into some other different gibberish form and then the encrypted information is transmitted. In the steganography, the information is embedded in an image file and the image file is transmitted. This paper focuses on the quality of consolidating cryptography and steganography routines to upgrade the security of correspondence over an open channel. [7]

Manoj Kumar Pandey (2013) et al present that Data security is one of the important aspects of data communication. The confidential data being sent via electrical media is very sensitive, which can be accessed for malicious purpose. The conventional methods of encryption can only maintain the data security so modern cryptography is very much needed to enhance the data security, so need of developing new concept and new cryptography is demand of the hour. Therefore it is necessary to apply efficient encryption technique to enhance data security. This paper mainly focuses on the different kind of encryption techniques that existing. [3] Data security is one of the import aspects of communication. Security of data can be achieved using the art of cryptography. There are many algorithms available for cryptography but the selection of one of the best algorithm is also very important. The encryption algorithm can be particular based on data kind being communicated and channel kind through which information is being communicated. In this paper, it has been overviewed that the current takes a shot at the encryption methods. Those encryption techniques are analyzed well to enhance the data security. As the day passes modern encryption is needed to promote the data security. The study of multiphase encryption techniques enhances the data security but multiphase techniques must also be reviewed for security purpose.

Factors	AES	3DES	DES	BLOW FISH
Key length	128,192, 256	K1,k2,k3 168 bits	56 bits	32-448 bits(128 by default)
Cipher type	Symmetric block cipher	Symmetric	Symmetric	Symmetric
Block size	128,192, 256	64	64	64
Created by	Joan Daemen & Vincent Rijmen in 1998	IBM in 1978	IBM in 1975	Bruce Schneier in 1993
Possible Keys	2 ¹²⁸ , 2 ¹⁹² 2 ²⁵⁶	2 ¹¹² or 2 ¹⁶⁸	2 ⁵⁶	2 ³² to 2 ⁴⁴⁸

Algorithm Structure	Substitution Permutation Network	Fiestel Network	Fiestel Network	Fiestel Network
Rounds	9,11,13	48	16	16
Effectiveness	Effective in Both S/W & H/W	Slow Especially in S/W	Slow	Efficient in S/W
Attacks	Side Channel Attacks	Theoretically possible	Brute Force Attack	Not Yet

Table 1: Comparison for Encryption Algorithm

VII. BIOMETRICS IN SECURE AUTHENTICATION

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. The physical characteristics of a person like finger prints, hand geometry, face, voice and iris are known as biometrics.

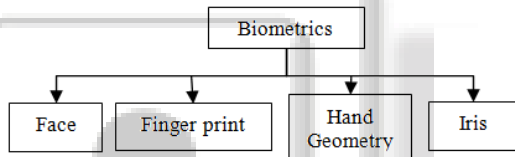


Fig. 6: Types of Biometrics System

VIII. CONCLUSION

In Data communication, encryption algorithm plays an important role. Our research work surveyed the existing encryption techniques like AES, DES and RSA algorithms technique. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. In this wireless world nowadays, the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. In this paper, it has been surveyed about the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. In future work, enhance the security authentication by using cryptography technique with biometrics for more security.

REFERENCES

[1] E. Surya and C.Diviya,” A Survey on Symmetric Key Encryption Algorithms”, E Surya et al , International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477

[2] I. Venkata Sai Manoj, “Cryptography and Steganography”, International Journal of Computer Applications (0975 –8887), Volume 1 – No.12

[3] Manoj Kumar Pandey and Mrs. Deepy Dubey,” Survey Paper: Cryptography The art of hiding Information”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12, December 2013

[4] Mitali, Vijay Kumar and Arvind Sharma,” Survey on Various Cryptography Techniques”, International Journal of Emerging Trends & Technology in Computer Science (IJETCS) Web Site: www.ijetcs.org Email: editor@ijettes.org Volume 3, Issue 4, July-August 2014, pp: 307-312.

[5] Pranab Garg, Jaswinder Singh Dilawari,” A Review Paper on Cryptography and Significance of Key Length”, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on “Emerging Trends in Engineering” ICETIE 2012,pp:88-91.

[6] Shivangi Goyal,” A Survey on the Applications of Cryptography”, International Journal of Science and Technology Volume 1 No. 3, March, 2012, pp:137-140.

[7] A. Joseph Raphael and Dr.V Sundaram,” Cryptography and Steganography – A Survey”, A.Joseph Raphael, Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630