INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 4255 Cities in 176 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE: The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS: Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS: Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.

6. **KEYWORDS: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e. **grammatical, spelling** or **punctuation.** It must be thoroughly edited at your end*.

9. **HEADINGS: All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS: All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION
REVIEW OF LITERATURE
NEED/IMPORTANCE OF THE STUDY
STATEMENT OF THE PROBLEM
OBJECTIVES
HYPOTHESIS (ES)
RESEARCH METHODOLOGY
RESULTS & DISCUSSION
FINDINGS
RECOMMENDATIONS/SUGGESTIONS
CONCLUSIONS
LIMITATIONS
SCOPE FOR FURTHER RESEARCH
REFERENCES
APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SURVEY OF VARIOUS CRYPTOGRAPHIC TECHNIQUES

AASHA M. VANVE
STUDENT
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

ABIRAMI SIVAPRASAD
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

ABSTRACT

Cryptography and encryption have been used for secure communication for thousands of years. Throughout history, military communication has had the greatest influence on encryption and the advancements thereof. The need for secure commercial and private communication has been led by the Information Age, which began in the 1980's. Although the Internet had been invented in the late 1960's, it did not gain a public face until the World Wide Web was invented in 1989. The World Wide Web is an electronic protocol which allows people to communicate mail, information, and commerce through a digital medium. This new method of information exchange has caused a tremendous need for information security. A thorough understanding of cryptography and encryption will help the people to develop better ways to protect valuable information as technology becomes faster and more efficient.

KEYWORDS
Cryptography, Encryption, Security.

1. INTRODUCTION

1.1 OVERVIEW OF CRYPTOGRAPHY

Cryptography a modern encryption technology, comprising of different mathematical processes involving the application of formulas (or algorithms) was conventionally designed to secure discretion of military and diplomatic communications. With the Rapid growth of Information Technology and science of encryption, an innovative area for cryptographic products has stimulated. Cryptography plays a major role in securing data. It is used to ensure that the contents of a message are confidentially transmitted and would not be altered. Network security is most vital component in information security as it refers to all hardware and software function, characteristics, features, operational procedures, accountability, access control, and administrative and management policy. Cryptography is central to IT security challenges, since it underpins privacy, confidentiality and identity, which together provide the fundamentals for trusted e-commerce and secure communication. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication.

1.1.1 DEFINITION

1. Cryptography: It is defined as the subdivision of cryptology in which encryption/decryption algorithms are designed, to guarantee the security and authentication of data which passes over the interconnected networks.
2. Computer Security: Generic name for the collection of tools designed to protect data and to thwart hackers.
3. Network Security: Measures to protect data during their transmission.
4. Internet Security: Measures to protect data during their transmission over a collection of interconnected networks.

1.2 OBJECTIVES OF CRYPTOGRAPHY

In data and telecommunications, cryptography is necessary when communicating over any un trusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

1. CONFIDENTIALITY

- The principle of confidentiality specifies that only the sender and the intended recipients should be able to access the contents of a message.
- User A sends a message to user B and another user C gets access to this message, without the permission of A and B. This type of attack is called as interception.

2. AUTHENTICATION

- It helps to establish proof of identities; it ensures that the origin of an electronic message or document is correctly identified.
- User C sends an electronic document over the internet to B But C posing as User A, sending a fund transfer request(From A to C's a/c) to bank B. Bank transfer the funds from A to C's a/c ,it would think that user A has requested the fund transfer. This type of attack is known as fabrication.

3. INTEGRITY

- When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, i.e. integrity of the message is lost.
- Suppose you write a cheque for Rs.1000 to pay the goods. However, when you see your next account statement that the cheque is resulted in a payment of Rs.10000.This is the case for loss of message integrity. This type of attack is known as modification.

4. NON-REPUDIATION

- User sends a message and later on refuses that he had sent the msg.
- User A send a fund transfer request to bank B over the internet. After the bank perform the fund transfer as per A's instruction. A could claim that he never sent the funds transfer instruction to the bank i.e. A denies the fund transfer instruction.
- Thus non-repudiation defeats such possibilities of denying something, having done it.

5. ACCESS CONTROL

- It determines who should be able to access what.
- It means we should be able to specify that user A can view the records in the database but cannot update them.
- It is related to two areas: role management and rule management.
- Role management concentrates on the user side (which user can do what).
- Rule management focus on resources side (which resources is accessible and under what circumstances).

6. AVAILABILITY

- It states that resources should be available to authorized parties at all times.
- For example: Due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server computer B.
- This would defeat the principle of availability. Such an attack is called as interruption.

1.3 NEED OF CRYPTOGRAPHY

- Information Security requirements have changed in recent times.
- Traditionally provided by physical and administrative mechanisms.
- Computer use requires automated tools to protect files and other stored information.
- Use of networks and communications links requires measures to protect data during transmission.

1.4 SECURITY ATTACK

1.4.1 MODERN NATURE OF ATTACKS

1. AUTOMATING ATTACKS

- The speed of computers makes several attacks.
- Someone creates machines that can produce counterfeit coins producing so many coins on a mass scale which will affect the economy.
- This is quite different with computers. Attacker can steal a half a dollar from million bank accounts in few minutes which would give him a half million dollars possibly without any major complaints.

2. PRIVACY CONCERN

- Collecting the information about the people and later misusing it is turning out to be a huge problem.
- Every company (shopkeepers, banks, airlines, insurers) are collecting and processing the huge amount of information about us, without we realizing when and how it is going to be used.

3. DISTANCE DOES NOT MATTER

- Thieves would earlier attack banks because they had money.
- Now Money is in digital form inside computers and moves around by using computer network.
- And it is very easy and cheaper to attack on the computer systems of the bank by sitting at the home.

1.4.2 TYPES OF SECURITY ATTACKS

General Types of Security Attack are:

1. CRIMINAL ATTACK

- The main aim of the attacker is to maximize financial gain by attacking computer systems.

2. PUBLICITY ATTACK

- An attacker wants to see their names appear on television, news channel and newspaper.
- They are not hardcore criminals.
- Such as students in universities or employees in large organizations, who seek publicity by adopting a Nobel approach of attacking computer systems.
- One form of publicity attack is to damage the webpages of a site by attacking it.
- One of such attack was occurred on the US department of Justice's website in 1996.

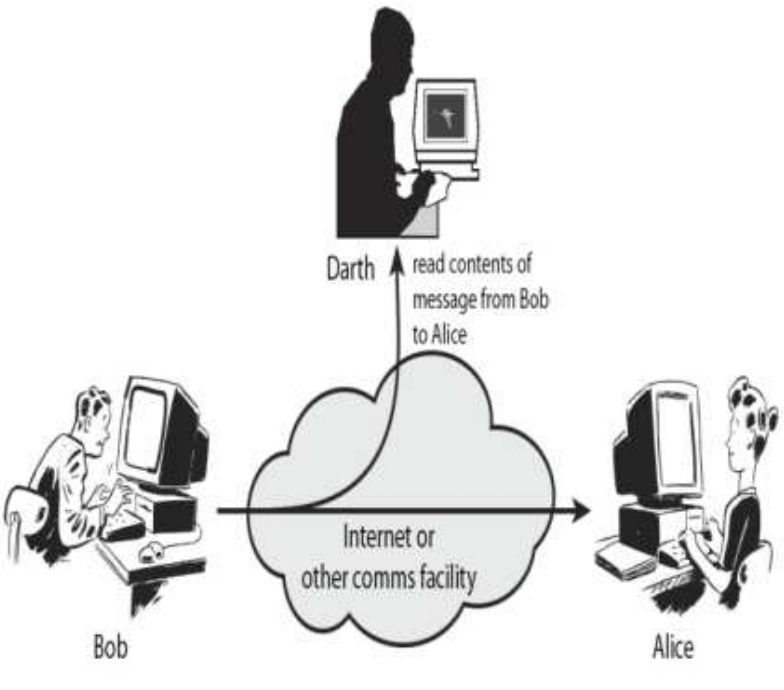
3. LEGAL ATTACK

- The attacker tries to make the judge or the jury doubtful about the security of a computer system.
- The attacker attacks the computer system and the attacked party manages to take the attacker to the court.
- In court attacker tries to convince the judge that there is weakness in the computer system and he has done nothing wrong.
- The aim of the attacker is to exploit the weakness of the judge and the jury in the technological mattes.

Main types of Security Attack are:

1. Passive Attacks

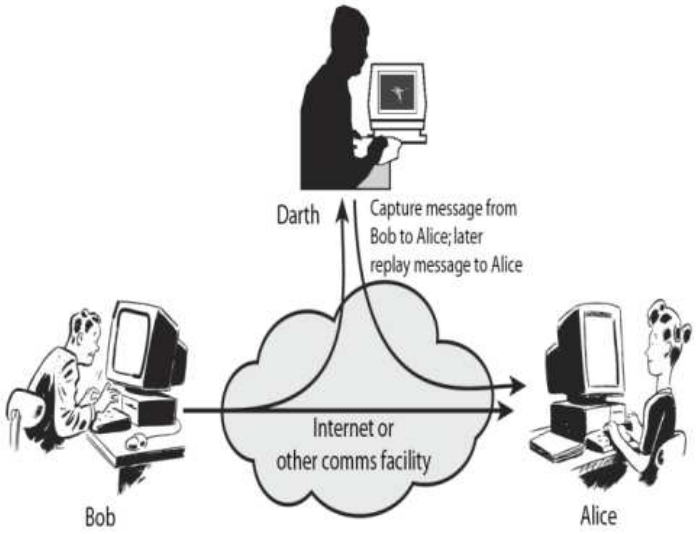
FIGURE 1: PASSIVE ATTACKS



- Eavesdropping or monitoring of data transmissions to obtain message contents.
- Passive attacks do not involve any modification to the contents of an original message.
- Thus the general approach to deal with the passive attack is to think about the prevention rather than detection or corrective actions.
- It is further classified into two sub categories. That is Release of message contents and Traffic analysis.
- Release of message contents: When we send confidential email message to our friend we desire that only he should be able to access it. Otherwise the contents of message are released against our wishes to someone else.
- Traffic analysis: We encode messages using a code language so that the only desired party understands the message. It may happen that a passive attacker could try to figure out similarities between them to come with some sort of pattern that provides him some clues regarding the communication takes place. Such attempts of analysing the encoded messages to come with likely patterns are the work of the traffic analysis attack.

2. ACTIVE ATTACKS

FIGURE 2: ACTIVE ATTACKS



- Active attacks are based on the modification of the original massage in some manner or the creation of false message.
- These attacks can be in the form of interruption, modification and fabrication.
- Trying to pose as another entity involves masquerade attacks.
- Masquerade is a type of attack where the attacker pretends to be an authorized user of a system to gain access to it.
- Modification attack can be classified into replay attacks.
- In this a user captures a sequence of events or some data units and resend them and alteration of messages.
- It involves some changes to the original message.

2. REVIEW OF LITERATURE

2.1 BASIC CONCEPTS OF CRYPTOGRAPHY

1. CRYPTOGRAPHY

- Cryptography is the study of Secret (crypto) writing (graphy).
- Concerned with developing algorithms.
- Conceal the context of some message from all except the sender and recipient (privacy or secrecy).
- Verify the correctness of a message to the recipient (authentication).
- It is the art and science of achieving security by encoding messages to make them non readable.

2. CRYPTANALYSIS

- It is the technique of decoding the messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

3. CRYPTOLOGY

- It is the combination of cryptography and cryptanalysis.
- That is: Cryptography + Cryptanalysis = Cryptology.

4. CIPHER

- An algorithm for transforming an intelligible message into unintelligible by transposition, substitution, or some other techniques.

5. PLAIN TEXT

- It is a message in clear text which is understood by human.

6. CIPHER TEXT

- When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

7. ENCIPHER (ENCODE)

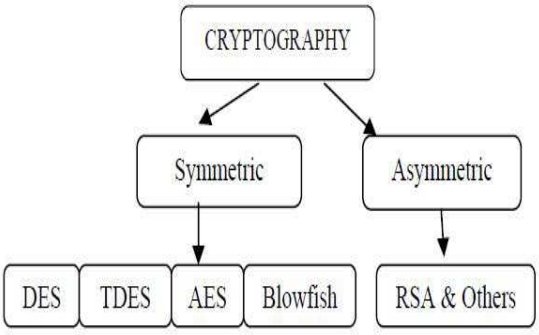
- The process of converting plaintext to cipher text.

8. DECIPHER (DECODE)

- The process of converting cipher text back into plaintext.

2.2 EXISTING TECHNIQUES OF CRYPTOGRAPHY

FIGURE 3: CLASSIFICATION OF CRYPTOGRAPHY



On the basis of number of keys Cryptographic algorithms are divided into two parts.

1. Symmetric Key Cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as Symmetric Key Cryptography. It is also called as Secret Key Cryptography (SKC).
2. Asymmetric Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is called Asymmetric Key Cryptography. It is also called as Public Key Cryptography (PKC).

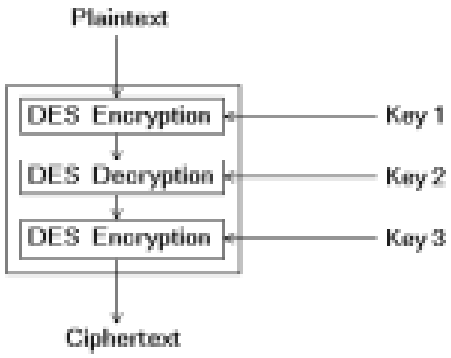
2.2.1 TYPES OF SYMMETRIC KEY CRYPTOGRAPHY

1. DES (DATA ENCRYPTION STANDARD)

It is a symmetric algorithm, means same key is used for encryption and decryption. DES is a block encryption algorithm. It uses one 64 bit key. Out of 64 bits, 56 bits used as independent key, which determine the exact cryptography transformation and 8 bits are used for error detection. The main operations are permutation and substitution. Bits permutation and substitution are performed in one round of DES. Six different permutation operations are performed both in key expansion and cipher part. Decryption process of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The drawback of this algorithm is, it can be easily prone to Brute force Attack. It is easy for the hacker to break the key by applying all possible combinations. In DES, there are only 2^256 possible combinations which are easy to crack. So DES is not secure.

2. 3DES (TRIPLE DATA ENCRYPTION STANDARD)

FIGURE 4: 3DES ENCRYPTION



Triple DES is replacement for DES due to advances in key searching. 3DES uses three rounds of DES encryption and has a key length of 168 bits. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt-Encrypt(EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message..

C(t) = Ek1(Dk2(Ek3(t))) (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 and 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) = Ek1(Dk2(Ek3(t))) (2)

TDES algorithm with three keys requires 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combinations, so TDES is a strongest encryption algorithm. The disadvantage of this algorithm it is too time consuming.

3. AES (ADVANCED ENCRYPTION STANDARD)

AES is replacement of DES. AES is a variable bit block cipher and uses variable key length of 128,192 and 256 bits. In AES, there are number of processing rounds. These rounds are based on the key size. If the key length is 128 bits, AES will perform nine processing rounds. If key is of 192 bits, AES perform 12 rounds and if the key size is 256 bits then AES perform 14 processing rounds. Each processing round involves four steps:-

- Substitute byte: A non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift rows: A transposition step where each row of the state is shifted cyclically a certain number of steps.
- Mix column: A mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add round key: Each byte of the state is combined with the round key using bitwise XOR.

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

4. BLOWFISH

Blowfish is a 64 bit block cipher and have variable length key from 32 bit to 448 bits. This algorithm has two parts – key expansion and data encryption. The key expansion part converts 448bit key into 468bytes A P array of size 18 and four S boxes whose size is 256, each of which are initialized to hexadecimal digits of π. XOR each entry in P array and S boxes with 32 bits of the key. There are 16 rounds of data encryption. In each round a 32 bit sub key is XORed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish. Now, this result becomes rightmost 32 bits for the next round and the output of F function is XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for next round and so on. The f function is distinguishing feature of Blowfish. In Blowfish, key length is 448 bits, s it requires 2^448 combinations to examine all keys. The advantage of this algorithm is, it is simple to implement as all operations are XOR and addition.

2.2.2 TYPES OF ASYMMETRIC KEY CRYPTOGRAPHY

1. RSA

RSA is most widely used public-key cryptosystem. It provides data confidentiality, key exchange and digital signature. The strength of RSA is factoring large numbers. It is a block cipher. In RSA, the plaintext and cipher text are integers between 0 and n-1 for some n. The description of the RSA algorithm is as follows. Plaintext is encrypted in blocks, with each block having a binary value less than some number n.

Public key components:

n = product of two large primes, p and q

e = a random number relatively prime and less than (p-1) (q-1)

Primary key components:

D = e-1 mod ((p-1) (q-1)), the multiplicative inverse of mod ((p-1) (q-1))

Encryption:

C = Me mod n

Decryption:

M = Cd mod n

Digital Signature:

S = Md mod n

M = Se mod n = Med mod n (to verify the signature)

The following requirements must be met for RSA to be satisfactory.

1. p and q , two large primes must remain secretive.
2. It is possible to find value of n, e, d such that,

Med mod n for all M<n.

3. It is infeasible to determine d, given e and n.
4. It is easy to calculate me and C for all values of M<n.

2. OTHER ASYMMETRIC KEY ALGORITHM

Other asymmetric key algorithms are used in conjunction with RSA. These other algorithms have their limitations. These algorithms are Diffie–Hellman, Digital Signature Algorithm, ElGamal and Elliptic Curve Cryptography. The disadvantage of Diffie-Hellman (DH) algorithm is that it is not as versatile as RSA and key generation might be too computationally expensive for the mobile device. Digital Signature Algorithm (DSA) is not as versatile as RSA. Another problem is that the key varies from 512 to 1024 bits, so requiring a strong key size beyond 1024 bits is not possible. DSA is slower than RSA in terms of signature verification. In ElGamal, the cipher text generated is twice the size as the plaintext; therefore it is not suitable in an environment with high latency and low bandwidth. ECC provides equal security for a smaller key size, thereby reducing processing overhead.

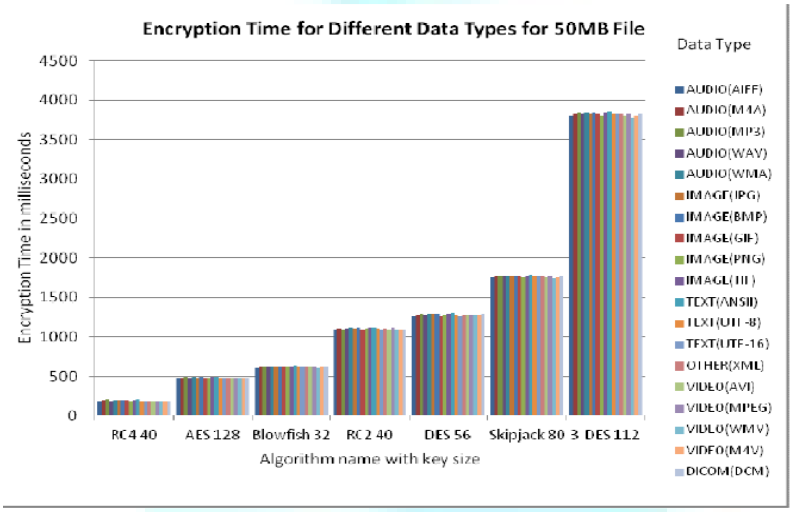
3. ANALYSIS

3.1 ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES

3.1.1 FILES WITH DIFFERENT DATA TYPES

This study has taken to check whether the encryption has dependency on type of data. Different data type files like audio, image, textual and video of nearly 50MB in size are chosen and encryption time of different cipher algorithms is calculated for these data types. For all executions of a specific cipher algorithm, varying parameter is data type and constant parameters are key size and block cipher mode. Key size and block mode are at kept at bare minimal parameters. The key size of AES, DES, and 3-DES, RC2, Blowfish, Skipjack, and RC4 are kept at minimum values as 128, 56, 112, 40, 32, 80 and 40 bits respectively. Block cipher mode used is ECB with PKCS#5 padding scheme. Figure shows the execution time of the algorithms for different data type files.

FIGURE 5: ENCRYPTION TIME VS. CIPHER ALGORITHM FOR FILES OF DIFFERENT DATA TYPE



Observation: In Figure it can be clearly seen that encryption time for all the data type is almost same. The result shows that the encryption time does not vary according to the type of the data. Encryption depends only on the number of bytes in the file and not on the type of file. Encryption time of AES is quiet low compared to other block ciphers. RC4 with key size 40 is fastest among the cipher algorithms tested.

3.1.2 DATA FILES OF SAME TYPE WITH DIFFERENT SIZES:

This case study is taken to ensure once again the observations obtained in case study 1. Case study 1 revealed that encryption time depends on number of bytes in the file. To ensure this another study is made in which different files (BMP and FLV) of same types but different sizes are given for encryption and their encryption time is calculated. For all executions key size and block mode are kept at bare minimal parameters. Figure 3.4 show the execution results for BMP and FLV file formats of different sizes respectively.

FIGURE 6: FILE SIZE Vs. ENCRYPTION TIME FOR BMP FILE OF DIFFERENT SIZES

File Type	Varying Parameters (Data Size)	Constant Parameters
BMP	10.7MB, 50MB, 100MB	Data Type, Key size
FLV	50MB, 100MB, 482MB	

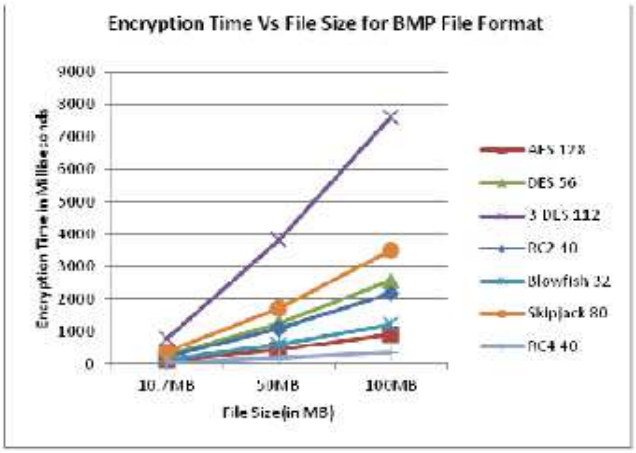
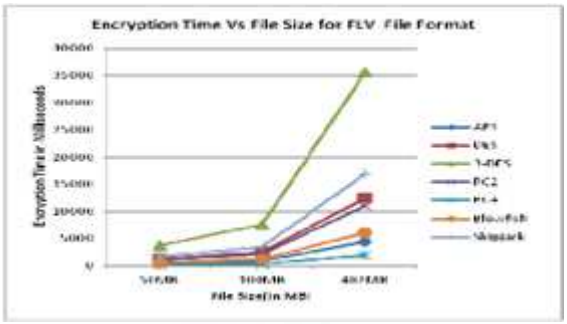


FIGURE 7: EXECUTION PARAMETERS FOR FILES OF DIFFERENT SIZE



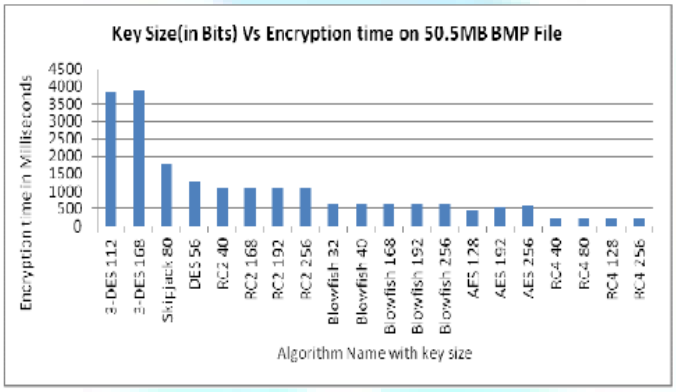
File Type	Size (In MB)	Encryption Time in Millisecond						
		AES 128	DES 56	3-DES 112	RC2 40	Blowfish 32	Skipjack 80	RC4 40
BMP	10.7	101	272	788	238	133	381	40
	50	455	1253	3804	1095	614	1729	198
	100	909	2595	7628	2189	1223	3505	372
FLV	50	456	1268	3810	1112	629	1731	196
	100	918	2586	7631	2224	1267	3515	360
	482	4518	12529	35654	11038	6087	16941	1972

Observation: For each encryption algorithm same parameters are used for files of different sizes. Figure 3.5 shows encryption time of different sizes of files of same type. From the results in figure we can find that the result for different size of data varies proportional to the size of data file. Encryption time increases as file size increases in multiples of data size.

3.1.3 ENCRYPTION ALGORITHMS WITH DIFFERENT KEY SIZES

This case study is to analyze the effect of changing the size of encryption key on encryption time. BMP file of 50.5MB is taken and different cipher algorithms are executed for different size of keys supported by them in ECB mode with PKCS#5 padding scheme. The various key sizes mentioned in Table 1 are used during experimentation. Figure 3.6 shows the result of execution for key size variation.

FIGURE 8: VARIATION OF KEY SIZES FOR DIFFERENT CIPHER ALGORITHMS



Observation: The execution results show that for all ciphers algorithms, the encryption time varies with the change in the size of the of the key. Encryption time increases with increase in key size for block ciphers. The variation in time is very small. AES dominates in the block cipher. RC4 is fastest among all algorithms tested.

From the simulated results it is concluded that encryption time is does not dependent upon data type and date density of the file. The research revealed that; encryption only depends upon the number of bytes present in the file. It also revealed that encryption time and data size is proportional to each other. As the size of data increase the encryption time also increase proportional to data size and vice versa. For all block cipher algorithms that are analyzed, with increase in key size, encryption time also increases, but reduces with increase in key size for stream cipher like RC4. AES is appears to be fastest block cipher with encryption rate of 108MB/sec at bare minimal parameter, but RC4 stream cipher with encryption rate of 270MB/sec comes out to be fastest among all analyzed cipher algorithms.

3.2 CONSTRAINTS FOR SELECTING RIGHT CRYPTOGRAPHIC SCHEME

The selection of right cryptographic technique relies on following constraints:

1. TIME

How much time will be needed for encrypting and decrypting the data and how much time is need to fulfill the prerequisites before starting an encryption how much time is need to fulfill the pre-requisites before starting an encryption.

2. MEMORY

How much memory will be needed especially in case of small devices like PDAs, smart cards, RFID tags.

3. SECURITY

Selected encryption scheme should meet the confidentiality, integrity (authentication, non-repudiation) and availability.

4. NATURE OF DATA

Nature of data means the communicating information is how much confidential or important. If the information is small in size and not too much important; then any encryption scheme is suitable. If information is highly secret or important then joint hybrid combination of symmetric + asymmetric scheme will be suitable.

5. TYPE OF DATA

In case of video data the privacy is more valuable and considerable constraint. If the data is small and in video format the previous described constrains (Time, memory, security) suggest the use of asymmetric scheme but this selection is not sufficient because the third party especially in case of Identity based Public Key Cryptography (ID-PKC) can view the video clip as they have all information (key(s), encrypted data). So in this case the privacy is nothing. That's why the type of data constraint is highly important constraint which should not be neglected in case of right selection of cryptographic scheme. If data type is confidential multimedia (personal video clip) then the symmetric scheme is good but hybrid encryption method (symmetric + asymmetric) can provide all security objectives.

3.3 PERFORMANCE FACTORS OF CRYPTOGRAPHIC ALGORITHMS

Various important factors on which performance of cryptographic algorithms depend are:

1. TUNABILITY

It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

2. COMPUTATIONAL SPEED

In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

3. KEY LENGTH VALUE

In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.

4. ENCRYPTION RATIO

The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation.

5. SECURITY ISSUES

Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In the analysis cryptographic security is in three levels: low, medium and high.

3.4 COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC TCHNIQUES

TABLE 1: COMPARATIVE ANALYSIS OF VARIOUS CRYPTOGRAPHIC TECHNIQUES

Distinguishing Parameters	DES	3DES	AES	Blowfish	RSA
Designers	IBM	IBM	Vincent RijmenJoan Daemon	Bruce Schneier	Ron Rivest, Adi Shamir, and Leonard Adleman
Published in	1977	1978	1998	1998	1977
Cipher Type	Symmetric	Symmetric	Symmetric	Symmetric	Asymmetric
Key Used	Same key used for Encryption and Decryption	Same key used for Encryption and Decryption	Same key used for Encryption and Decryption	Same key used for Encryption and Decryption	Different key used for Encryption and Decryption
Key Sizes	56 bits (+8 parity bits)	168 bits	128,192,256 bits	32-448 bits	1024-4096 bits
Block sizes	64 bits	64 bits	128 bits	64 bits	Blocks having binary values less than some number n
Structure	Balanced Feistel Network	Feistel Network	Substitution Permutation Network	Feistel Network	Mathematical based
Rounds	16	48	10, 12 or 14 (depending on key size)	16	1
Attacks	Brute Force Attack	Theoretically possible	Side channel attacks	Not yet	A 768bit key has broken
Security	Proven Inadequate	Still Insecure	Secure	More Secure	Secure
Speed	Low	Moderate	High	Very high	High

4. CONCLUSION

Cryptography is an emerging technology which is important for network security. Some well-known cryptographic algorithms have been analyzed in this report. This report gives a detailed study of the popular symmetric key encryption algorithms such as DES, Triple DES, AES, Blowfish and asymmetric key encryption algorithms such as RSA etc. AES is appears to be fastest block cipher with encryption rate of 108MB/sec at bare minimal parameter, but RC4 stream cipher with encryption rate of 270MB/sec comes out to be fastest among all analyzed cipher algorithms. Asymmetric encryption algorithms are more secure than symmetric key algorithms.

REFERENCES

BOOKS

1. Cryptography and Network Security by Atul Kahate, second edition Tata McGrawHill.
2. Cryptography and Network Security Principles and Practice By William Stallings. Fifth Edition. Pearson Education.
3. Cryptography Theory and Practice By Douglas Stinson, CRC Press.

JOURNAL AND OTHER ARTICLES

4. Anjali Patil, Rajeshwari Goudar, International Journal of Scientific and Tehnology Research Volume 2, Issue 8, August 2013 “A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices”.
5. Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh at International Journal of Advanced Engineering Technology, “Comparative Analysis of Cryptographic Algorithms”.
6. Mr. Mahavir Jain, International Journal Of Core Engineering & Management (IJCEM) Volume 1, Issue 3, June 2014, “Implementation Of Hybrid Cryptography Algorithm”.
7. Nikita & Ranjeet Kaur, International Journal of Research in Engineering & Technology (IMPACT: IJRET), Vol.2, Issue 5, May 2014, “Survey on secret key encryption technique”.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals