# 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, Polandwith 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 2477 Cities in 159 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

## ASSOCIATE EDITORS

## TECHNICAL ADVISOR

## FINANCIAL ADVISORS

## LEGAL ADVISORS

## SUPERINTENDENT

# CALL FOR MANUSCRIPTS

Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Education, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; 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; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor 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; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

# 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/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)**

**DEAR SIR/MADAM**

Please find my submission of manuscript entitled '____________________________________________' for possible publication in 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 author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

**NAME OF CORRESPONDING AUTHOR**:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

**NOTES**:

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

b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
**New Manuscript for Review in the area of** (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/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 required to be below **500 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 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 separate mail to the journal.

2. **MANUSCRIPT TITLE**: The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS**: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **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 stops at the end.

6. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT**: The main text should follow the following sequence:

   INTRODUCTION

   REVIEW OF LITERATURE

   NEED/IMPORTANCE OF THE STUDY

   STATEMENT OF THE PROBLEM

   OBJECTIVES

   HYPOTHESES

   RESEARCH METHODOLOGY

   RESULTS & DISCUSSION

   FINDINGS

   RECOMMENDATIONS/SUGGESTIONS

   CONCLUSIONS

   SCOPE FOR FURTHER RESEARCH

   ACKNOWLEDGMENTS

   REFERENCES

   APPENDIX/ANNEXURE

   It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **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.

11. **EQUATIONS**:These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **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**. 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 parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

**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, 19–22 June.

**UNPUBLISHED DISSERTATIONS AND THESES**

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, KurukshetraUniversity, 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 Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

# METHODS OF DATA SECURITY USED IN COMPUTER NETWORK

*ZOBAIR ULLAH*
*LECTURER*
*SAM HIGGINBOTTOM INSTITUTE OF AGRICULTURE*
*TECHNOLOGY AND SCIENCES*
*ALLAHABAD*

## ABSTRACT

*The paper is intended to discuss the need of data security in computer network and to explore the different methods available in this connection. The paper basically deals with the different methods and techniques available for securing data to a large extent on a computer network.*

KEYWORDS
Data security, Authentication, Authorization, Cryptography, Symmetric encryption, Asymmetric encryption, Hashing and Digital signature

## 1.0 INTRODUCTION

Nowadays man has been increasingly becoming dependent on internet and web surfing. People are really enjoying this technology because of the fact that it has increased the work efficiency at a tremendous rate. But at the same time, the growing popularity of this technology in public domain led some serious issues like virus infection, tampering of data, spooling and leakage of private information to some unauthorised hands. Therefore, in order to provide data security data encryption is necessary and mandatory. The paper lucidly introduces the major security issues and how these can be dealt that arises while sending data or message from one point to another on a computer network.

### 1.1 DEFINITION

**Data security** refers to the practice of keeping data protected from tampering, corruption and unauthorised access.

### 1.2 IMPORTANCE OF DATA SECURITY

Data security is needed to ensure privacy of personal or corporate/business data. Data security methods/techniques prevent virtual attack, physical attack, flexibility and transparency of data in a firm. The information like client information, payment information, personal files and bank account details need standard security system to a large extent because of the fact that these information can be hard to replace and potentially dangerous if it falls into the wrong hands like hackers or predators.

## 2.0 METHODS OF DATA SECURITY USED IN COMPUTER NETWORK ARE AS ENUMERATED

### 2.1 AUTHENTICATION

It refers to the process of identifying an individual, usually based on a username and password. In general, it verifies “who you are”. The process of authentication is usually required to login into a UNIX server or accessing mail server using POP3 and SMTP client. This method facilitates username/password validation using users own premises Active Directory/LDAP server. Authentication service is installed as a virtual appliance and communicates with user’s local directory using LDAP over SSL. When the user is authenticated, a session token is usually placed into the user’s browser. Usually, PAM (Pluggable Authentication Modules) is used as low authentication schemes into a high level application programming interface (API).

### 2.2 TYPES OF AUTHENTICATION

- **User authentication** -------- refers to the process of determining that a user is who he/she claims to be.
- **Entity authentication** ------- refers to the process of identifying an individual usually based on a username and password.

### 2.3 APPLICATION OF AUTHENTICATION IN DAILY LIFE

- Demanding voter ID or photo ID.
- Entering a country with a passport.
- Logging in to a computer.
- Using a confirmation e-mail to verify ownership of an e-mail address.
- Using internet banking system.
- Withdrawing cash from an ATM.

## 3.0 AUTHORIZATION

It refers to the process of giving individuals access to system objects based on their identity. In general, it verifies “what the user is authorised to do”. Here the user is allowed to login into the (UNIX) system but the user is restricted or not authorised to use or access browser or any other file system. Authorization is usually controlled at file system level.

## 4.0 CRYPTOGRAPHY

It refers to the practice and study of techniques for secure communication in the presence of third parties (called adversaries). The term cryptography comes from Greek words meaning “hidden writing”. It is the science of hiding information so that unauthorised users cannot read it. Cryptography is synonymous with the term data encryption which means the conversion of information from a readable state to apparent nonsense.

### 4.1 DATA ENCRYPTION

It refers to mathematical calculations and algorithmic schemes that transform plaintext into cipher text, a form that is non readable and unusable to unauthorized parties. Modern cryptography is heavily based on mathematical theory and computer science practice. These cryptographic algorithms are to break in practice by any adversary. Cryptographic algorithms and analysing protocols are designed/ constructed to overcome the influence of adversaries. Cryptography or data encryption is directly related to various aspects of information security such as data confidentiality, data integrity, authentication and non repudiation. Historically, encryption systems used symmetric cryptography. As far as computer network is concerned, data encryption is absolutely necessary because it transmits sensitive data over unsecure mediums like the internet.

### 4.2 TYPES OF ALGORITHMS USED FOR DATA ENCRYPTION ARE:

- Symmetric encryption or cryptography and
- Asymmetric encryption or cryptography

Now, each one is discussed as under:

**4.2.1 SYMMETRIC CRYPTOGRAPHY ------** refers to encryption methods in which both the sender and receiver share the same key. It is also known as secret key cryptography. Symmetric cryptography uses the same key for both encryption and decryption.

**KEY ------** In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Therefore, the key has the ability to encrypt or decrypt the data.

**KEY MANAGEMENT** ------ refers to the secure administration of keys to provide them to users where and when they are required.

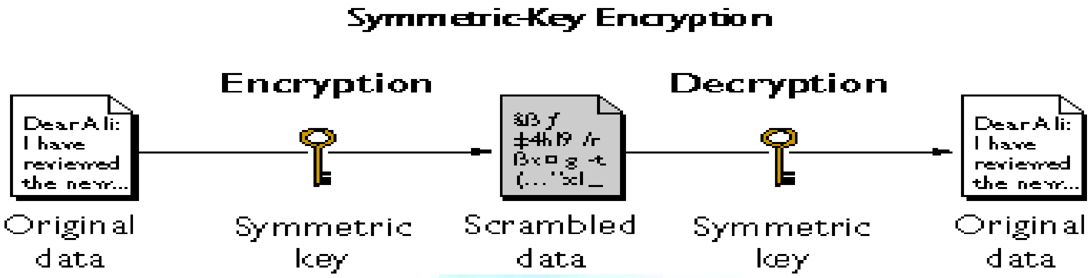
**CIPHER TEXT** ---- Cryptography converts readable data or clear text into encoded data called cipher text.

**4.2.2 Types of symmetric key cryptography (data encryption)**

- Block cipher
- Stream cipher
- Hashing or cryptographic hash functions

**4.2.2.1 Block cipher** ----- refers to the method of encrypting text to produce cipher text. In this method cryptographic key and algorithm are applied to a block of data. Block ciphers generally convert a fixed length block of plaintext into cipher text of the same length, which is under the control of the secret key. Decryption is effected using the reverse transformation and the same key.

**FIG. 1**



Different techniques used to cipher plaintext messages are:

- **ECB** ----- Electronic Code book
- **CBC** ----- Cipher block chaining
- **CFB** ----- Cipher feedback
- **OFB** ----- Output feedback mode

Block ciphers include DES, IDEA, AES, FEAL, SAFER, BLOWFISH, RIVEST CIPHER (RC) and SKIPJACK

**DES (DATA ENCRYPTION STANDARD)** -------- It is the main standard for encrypting data using symmetric algorithm. It is a widely used method of data encryption using a private (secret) key. Earlier it was difficult to break. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from this enormous number of keys. In this case both the sender and the receiver must know and use the same private key. DES applies 56 bit key to each 64 bit block of data. The process can run in several modes and involves 16 rounds or operations.

**APPLICATIONS OF DES** -------- ATM (Automated teller machine) encryption commonly used in banks, e-mail privacy and secure remote access.

**DEMERIT**

DES can be broken. DES is vulnerable or prone to brute force attack or exhaustive key search, a repeated trying of keys until one fits. Example FEAL

**IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM)** ------- refers to an iterative block cipher and uses 128 bit keys and eight rounds. This gives much more security.

**ADVANCED ENCRYPTION STANDARD (AES)** ----- This is the newest encryption standard which allows a maximum of 256 bits. AES has not been cracked. Therefore, it is widely used by the US government.

**FEAL** ------ Stands for Fast Data Encipherment algorithm (FEAL). Examples are FEAL-4, FEAL-8 and FEAL-N. They are very insecure.

**SAFER** ----- refers to a symmetric cipher coming with 40, 64 and 128 bit keys.

**BLOWFISH** ----- It is a combination of Fiestal network, key dependent S-boxes and a non invertible F function. It is considered as a strong open source symmetric algorithm.

**RIVEST CIPHER** ------ refers to a group of algorithms that can take on a variable block size, key size and number of rounds. The block size is generally dependent on the word size of the machine. For example, RC5 was designed to run on 32 bit processors. Some of the popular Rivest cipher are RC-2, RC-5 and RC-6.

**SKIPJACK** -------- refers to a symmetric cipher coming with 80 bit keys.

**64- BIT BLOCK CIPHER** ------- refers to the DES (Data Encryption Standard) that encrypts data 64 bits at a time.

**4.2.2.2 STREAM CIPHERS** ------ In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. For example, RC4. It is a widely used stream cipher.

**4.2.2.3 Hashing or cryptographic hash functions** ------ refers to the function that transforms data of arbitrary length into a smaller fixed length, more commonly known as a message digest. These cryptographic hash functions generally take a message of any length as input and output a short, fixed length hash. It can be used in a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. Hash algorithms are often generated by the DES algorithm to encrypt online banking transactions and other communications where messages can't afford to be corrupted. MD4 and MD5 are widely used hash function but now broken.

**WORKING OF HASHING ALGORITHMS** ----- this algorithm generally transforms a text string into an alphanumeric string. Hashes are typically referred to as one way hashes and are difficult to reverse. Usually hash values never need to be decoded, when a user log onto his/her computer. Then the hash value is compared with the hash value stored on the server. When hashing is done, the resulting hash is normally smaller than the original.

Some popular hashing algorithms are: SHA (Secure Hash algorithm) and MD (Message Digest) algorithms.

The following table lists different types of hashing algorithms:

**TABLE 1**

| Hash | No. of bits | Cracked | Developer | Introduced |
|---|---|---|---|---|
| SHA- 1 | 160 | Yes | NSA | 1995 |
| SHA- 2 | | None | NSA | 2000 |
| SHA- 256 | 256 | None | NSA | 2000 |
| SHA- 384 | 384 | None | NSA | 2000 |
| SHA- 512 | 512 | None | NSA | 2000 |
| MD- 2 | 128 | Yes | Ronald Rivest | 1989 |
| MD- 5 | 128 | Yes | Ronald Rivest | 1991 |
| HAVAL | 128 | No | Yuliang Zheng | 1992 |
| RIPEND- 320 | 320 | No | Hans Dobbartin | 1996 |
| Gost | 64 | No | Soviet union | 1970 |
| Whirlpool | 512 | No | Paulo Barreto | 2001 |

**USE OF HASH CODE**

- **Maintaining integrity of messages** ----- a hash code is generally used for comparison purposes to make sure that data has not been changed.
- A hash code is used as a digital signature for the data.

**Digital signature ------** refers to a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions to detect and prevent forgery or tampering.

**4.2.2.4 Advantages of symmetric cryptography**

- It is safe to send encrypted messages without fear of interception.
- Symmetric cryptography is much faster and is suitable for encrypting large amount of information.

**4.2.2.5 Disadvantage of symmetric cryptography**

- Key management
- As the number of user increases on a network, the number of keys required to provide secure communications among those user increases rapidly. For instance, a network of hundred users would require almost five thousand (500) keys.

**4.3.1 Asymmetric cryptography -----** refers to the encryption algorithms that involve a pair of relative keys to encode and decode messages. Generally, one key is used to encrypt data into cipher text while the other key is used to decrypt cipher text back into plaintext or clear text. This cryptography uses a pair of keys called a private key and a public key. The public key is generally used to encrypt data before sending it to the recipient. When the message is encrypted it becomes viewable only for the owner of the private key, which will allow him to decrypt the information. Also, asymmetric cryptography algorithms are commonly known as public key cryptography.

**4.3.2 Types of asymmetric cryptography**

**RSA (Rivest Shamir- Adleman) algorithm -----** refers to a message that can be securely signed by a specific sender. If the sender encrypts the message using their private key, then the message can be decrypted only using that sender's public key, authenticating the sender.

**PKI (Public Key Infrastructure) -------** refers to the most common public key cryptographic method used on the internet for authenticating a message sender. PKI enables users of an unsecure public network like internet to securely and privately exchange data and money through the use of a public key and a private key pair that is obtained through a trusted authority. This method provide for a digital certificate that can identify an individual or an organisation. A PKI includes the following:

- CA (Certificate authority) ------- is an individual or a person that generally issues and verifies digital certificates. A digital certificate means an electronic "credit card" that establishes users credentials when doing business or other transactions on the web. A digital certificate basically contains username, a serial number, expiration dates and a copy of the certificate holder's public key (used for encrypting messages and digital signatures).
- RA (registration authority) ------- is an individual or a person that generally acts as the verifier for the CA before a digital certificate is issued to a requestor.
- One or more directories where the certificates (with the public keys) are held.
- A certificate management system.

**4.3.3 Application of asymmetric encryption**

- **Making digital certificates -----** Here certificate refers to a package of information that identifies a user or a server, and contains information such as the organisation name, the organisation that issued the certificate, the user's e-mail address and country and the user's public key.

**4.3.4 Advantages of asymmetric key cryptography**

- It is used to solve the problem of delivering the symmetric encryption key to the bank in a secure manner.
- It is considered to be more secure encryption method as its private key is not shared.

**4.3.5 Disadvantages of asymmetric key cryptography**

- Public key cryptography is relatively slow and is only suitable for encrypting small amounts of information such as symmetric keys.
- It did not provide a comprehensive solution to the key management problem.

## 5.0 ADVANTAGES OF CRYPTOGRAPHIC METHOD

- In the past, Julius Caesar was credited with creating one of the earliest cryptographic systems to send military messages to his generals.
- Nowadays, banking, online shopping and even home users uses the method of cryptography to protect data.
- In computer, a web browser automatically encrypts data to prevent intruders from stealing and intercepting private communications.

## 6.0 MODERN CRYPTOGRAPHY APPLICATIONS

- ATM cards
- Computer passwords
- Electronic commerce

## 7.0 CONCLUSION

The paper defines, describes and explains the different cryptographic method and techniques available to encode or decode any text or message to provide reliable privacy and security.

## 8.0 ACKNOWLEDGEMENT

I would like to express my deep gratitude to people around me (especially students and computer users) who most often raise security issues whenever their message passes through public domain using computer. At last I would like to thank the great almighty who has given wisdom, strength and knowledge to visualise and explore things from grass root level and put on papers for the benefit of mankind and promote safe invention and new discoveries.

## REFERENCES

1. Biham,Eli and Alex Biryukov: An improvement of Davies Attack on DES. J. Cryptography 10(3): 195-206(1997)
2. Coppersmith, Don (1994). The data encryption standard (DES) and its strength against attacks. (IBM Journal of Research and Development, 38(3), 243-250).
3. Langford, Susan K, Martin E.Hellman: Differential Linear Cryptography. CRYPTO 1994: 17-25
4. Stallings, W. Cryptography and network security: principles and practices: Prentice Hall,2006, p.73
5. Thomas R. Johnson "American cryptology during the cold war, 1945-1989 Book in Retrenchment and Reform, 1972- 1980". United States cryptologic History 5 (3).

# REQUEST FOR FEEDBACK

**Dear Readers**

At the very outset, International Journal of Research in Computer Application and 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**

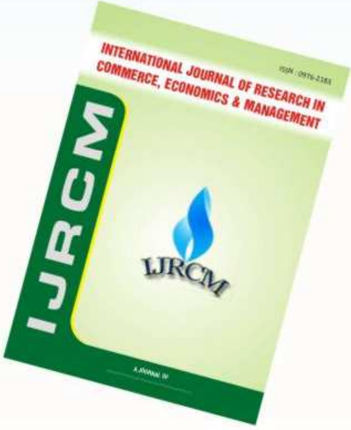
Sd/-

**Co-ordinator**

# 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


ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF

ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF