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., Google Scholar,
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 **5555 Cities** in **190 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

FORMER TECHNICAL ADVISOR

FINANCIAL ADVISORS

LEGAL ADVISORS

SUPERINTENDENT

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to the recent developments & practices in the areas of Computer Science & Applications;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 titled '____' for likely publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published anywhere in any language fully or partly, nor it is 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 inclusion of their 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/Post* :
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 :

* i.e. Alumnus (Male Alumni), Alumna (Female Alumni), Student, Research Scholar (M. Phil), Research Scholar (Ph. D.), JRF, Research Assistant, Assistant Lecturer, Lecturer, Senior Lecturer, Junior Assistant Professor, Assistant Professor, Senior Assistant Professor, Co-ordinator, Reader, Associate Professor, Professor, Head, Vice-Principal, Dy. Director, Principal, Director, Dean, President, Vice Chancellor, Industry Designation **etc**. ***The qualification of author is not acceptable for the purpose***.

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 the 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) Only the **Abstract 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 the manuscript, within two days of its 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 on 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 typed in **bold letters**, **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 Italic printing**, ranging between **150** to **300 words**. The abstract must be informative and elucidating 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 etc.

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 of 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 be in ***2000 to 5000 WORDS***, But the limits can vary depending on the nature of the manuscript.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self-explained, and the **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, left aligned with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word may 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 e.g. 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 may follow Harvard Style of Referencing. **Also check to ensure 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 italic printing. 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 before 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

A REVIEW ON NETWORK SECURITY AND CRYPTOGRAPHY

KIRAN SAHU
ASST. PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
GURU GHASIDAS VISHWAVIDYALAYA
BILASPUR

ABSTRACT

With the emergence of internet data Security has become critical for every sector since data is at the core of any organization. Moreover, as we are heading towards the age of digitization large amount of data is produced and transferred across the world every day. So in order to protect it various mechanisms and algorithms have been developed. Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Modern cryptography is heavily based on mathematical theory, computer science, practice and engineering discipline. In this paper an attempt has been made to review various network security principles, types of security attacks and cryptographic concepts and to achieve the aforesaid the data have been collected from reports published in journals, articles, magazines, books and online sources.

KEYWORDS

cryptography, decryption, digitization, encryption, internet, network security.

1. INTRODUCTION

Internet has proved to be a boon providing fast exchange of information across the globe. At the same time, it has posed serious threats to data security like unauthorised access and later its misuse which can end up everything. In this era of cut throat competition data plays a vital role in the success of any organization. So, network security has become a major challenge for the organizations. **Network Security** is the protection of data while transmission over the network whereas **Cryptography** is about constructing and analyzing techniques to provide data security. Network security consists of developing and implementing policies by network administrator to prevent unauthorised access, misuse, manipulation, and disruption of services of network. There are various aspects of network security:

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY

CONFIDENTIALITY- The principle of Confidentiality says that only authorised users i.e., the sender and the intended recipient should be able to access the message.

INTEGRITY- According to this principle, a message should be received by the receiver exactly in the same form as it was sent by the sender i.e. there should be no modification of the message in between.

AVAILABILITY-The principle of availability says that the message should be available to the recipient in proper time, when it is needed (without any delay).

These aspects of network security are central to cryptography. **Cryptography**, derived from Greek word 'Kryptos' ('hidden, Secret') is the science and art of transforming messages in order to make them secure and immune to attacks. Applications of cryptography include military communications, electronic commerce, ATM cards, and computer passwords. **Cryptanalysis** is the term used for the study of methods for decrypting the message without encryption details. The combined study of cryptography and cryptanalysis is called cryptology. ***Encryption*** is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext).**Decryption** is the reverse, converting the unintelligible ciphertext back to plaintext. A ***cipher*** is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The **key** is a secret (ideally known only to the communicants), usually a short string of characters, which is input to the encryption and decryption algorithms.

2. SECURITY ATTACKS

2.1. PASSIVE ATTACKS- This type of attack does not involve any change or modification of the message. The attacker's objective is to just obtain the information. Passive attacks may not harm the system but disclosure of information may harm the sender or receiver of the message. Since this type of attack does not involve any modification of the message they are difficult to detect and are more harmful.

Types of passive attacks:

a) Traffic Analysis
b) Snooping

TRAFFIC ANALYSIS- It involves monitoring of the online traffic by the attacker to guess the pattern of the message. The communicating entities never know that their message is being monitored.

SNOOPING- It involves unauthorised access of the information by the attacker which may later be misused.

2.2. ACTIVE ATTACKS- This type of attacks involve modification of data and may harm the system. They are easier to detect as compared to passive attacks.

Types of Active attacks:

a. MODIFICATION
b. MASQUERADE
c. REPLAY
d. NON-REPUDIATION
e. DENIAL OF SERVICE (DOS)

MODIFICATION- Some portion of the message is modified or deleted or delayed, which may harm the system.

MASQUERADE- Here one entity impersonates some other entity. The attacker may send some false message to the receiver pretending to be the actual sender or may pretend to be the actual receiver and receive some confidential information.

REPLAY- The attacker simply captures the message for some time and later retransmits it, thereby creating an unauthorised effect.

NON-REPUDIATION- This type of attack involves either the sender or the receiver. The means that the sender after sending the message may deny that he sent the message or the receiver may refuse that he received any message.

DENIAL OF SERVICE (DOS) - It involves disruption of the services of the server and destroying the whole network by the attacker. For example, the attacker may send some bogus requests to slow down the network and create unnecessary traffic or may divert the requests made to the server to some other route so that users are devoid of the services of the system. It ultimately destroys the whole system.

3. CRYPTOGRAPHY ALGORITHMS

3.1. SYMMETRIC KEY (PRIVATE KEY) CRYPTOGRAPHY – In symmetric key cryptography (**SKC**) a single key which is called 'shared secret key' is used for both encryption and decryption.

TYPES OF SKC ALGORITHMS

3.1.1. DATA ENCRYPTION STANDARD (DES): It was quite popular in the early days. DES was proposed by IBM in 1970 and published in 1977 by NIST. The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the 56 bits-secret key into a 64-bit ciphertext by means of permutation and substitution involving 16 rounds.

For any cipher, the most basic method of attack is a brute force, which involves trying each key until you find the right one. The length of the key determines the number of possible keys -- and hence the feasibility -- of this type of attack. Hence, it would take a maximum of 2^56, or 72,057,594,037,927,936, attempts to find the correct key. But many security experts felt the 56-bit key length was inadequate and messages encrypted using DES encryption are likely to be subjected to this kind of code-breaking effort. Even so, DES remained a trusted and widely used encryption algorithm through the mid-1990s. However, in 1998, a computer built by the Electronic Frontier Foundation (EFF) decrypted a DES-encoded message in 56 hours. So **National Institute of Standards and Technology (NIST)** in 2001 selected the **Advanced Encryption Standard (AES)** as a replacement for DES.

3.1.2 ADVANCED ENCRYPTION STANDARD (AES): AES is an SKC algorithm.It is a subset of the Rijndael cipher(ciphers with different key and block sizes) developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. AES encrypts and decrypts a block size of 128 bits. It uses 10, 12, or 14 rounds. The key size which can be 128 or 192 or 256, depends on the number of rounds. AES has 3 different versions AES-128, AES-192 and AES-256 with 10, 12 and 14 rounds respectively. But the round key size is always 128 bits.

3.1.3. IDEA- Although less visible than DES, the International Data Encryption Algorithm (IDEA) has been classified by some of the contemporary cryptographers as the most secure and reliable block-algorithm. Like DES, IDEA encrypts data in 64-bit input blocks; for each it outputs corresponding 64-bit cipher block. It employs the same algorithm for encryption and decryption, with a change in the key schedule during encryption. Unlike DES, IDEA employs 128-bit secret key and dominantly uses operations from three algebraic groups: XOR, addition modulo 2^{16}, and multiplication modulo $2^{16} + 1$. These operations are combined to make 8 computationally identical rounds followed by an output transformation resulting in the final ciphertext.

3.1.4. SAFER- SAFER stands for Secure and Fast Encryption Routine. It is a block cipher developed by Massey in 1993 for Cylink Corporation. It uses a 64 bit block size.

3.1.5. RIVEST CIPHERS (aka RON'S CODE): Named for Ron Rivest, a series of SKC algorithms.

RC1: Noted on paper, but not at all implemented.

RC2: A 64-bit block cipher using variable-sized keys intended to change DES.

RC3: Found to be breakable at some stage in development.

RC4: A stream cipher with variable-sized keys; it is broadly used in business cryptography products.

RC5: A block-cipher sustaining a variety of block sizes (32, 64, or 128 bits), key sizes, and quantity of encryption passes in excess of the data.

RC6: A 128-bit block cipher based upon, and an upgrading over, RC5;

3.1.6 BLOWFISH – It is an iterative block cipher developed by Bruce Schneier in 1993. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It’s definitely one of the more flexible encryption methods available.

3.2. ASYMMETRIC KEY CRYPTOGRAPHY (PUBLIC KEY) - As the name implies, it uses two different keys, public key and private key for encryption and decryption respectively.

3.2.1 RSA Algorithm- The most common public key algorithm is RSA named after its inventors Rivest, Shamir and Adleman. RSA uses 2 exponent e and d, where e is public and d is private.

The cipher text (say C) is calculated from plain text (say P) as:

$$\boxed{C=P^{e} \bmod n}$$

And, the reverse i.e. plain text (original message) is calculated as:

$$\boxed{P=C^{d} \bmod n}$$

The key generation procedure follows:

i. Select two primes p and q such that p ≠q

ii. Calculate n=p*q

iii. Calculate ϕ(n)=(p-1) * (q-1)

iv. Select e such that 1<e< ϕ(n) and GCD(e, ϕ(n))=1

v. Now calculate d such that ed mod ϕ(n)=1

vi. So our public key → (e, n) [TO BE ANNOUNCED PUBLICLY]

vii. And, our private key → d [TO BE KEPT SECRET]

3.2.2 RABIN Cryptosystem- Devised by M. Rabin, RABIN algorithm is a variation of the RSA algorithm in which e and d are fixed, e=2 and d=1/2.

The cipher text (say C) is calculated from plain text (say P) as:

$$\boxed{C=P^{2} \bmod n}$$

And, the reverse i.e. plain text (original message) is calculated as:

$$\boxed{P=C^{1/2} \bmod n}$$

In RABIN Cryptosystem public key is n and private key is the tuple (p, q). Everyone can encrypt the message using n but only the receiver can decrypt the message using p and q.

The key generation procedure follows:

i. Select 2 large primes p and q in the form of 4k+3 and p ≠q

ii. Calculate n=p*q

iii. Public key → n

iv. Private key →(p, q)

To encrypt a message only the public key *n* is needed. To decrypt a ciphertext the factors *p* and *q* of *n* are necessary.

3.2.3 DIFFIE-HELLMAN KEY EXCHANGE – Diffie-Hellman key agreement algorithm is one of the earliest public-key protocols for securely exchanging cryptographic keys over a public channel. It was developed by Dr. Whitfield Diffie and Dr. Martin Hellman in 1976. It is not for encryption or decryption, but it enables two parties who are involved in communication to generate a secret key for exchanging information confidentially.

The working of Diffie-Hellman key agreement can be explained as below:

1) Two communicating entities P1 and P2 agree on two large integers a and b such that 1< a< b.

2) P1 then chooses a random number i and computes I = $(a)^i$ mod b. P1 sends I to P2.
3) P2 then chooses a random number j and computes J = $(a)^j$ mod b. P2 sends J to P1.
4) P1 computes k1 = $(J)^i$ mod b.
5) P2 computes k2 = $(I)^j$ mod b.
6) We have k1 = k2 = **$(a)^{ij}$ mod b** and thus k1 and k2 are the secret keys for secure transmission.

3.2.4. ELGAMAL CRYPTOSYSTEM

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key exchange protocol.

The system parameters consist of a prime *p* and an integer *g*, whose powers modulo *p* generate a large number of elements, as in Diffie-Hellman. P1 has a private key *a* and a public key *y*, where **$y = g^a$ (mod p).** Suppose P2 wishes to send a message *m* to P1. P2 first generates a random number *k* less than *p.* He then computes $y_1 = g^k$ (mod p) and $y_2 = m$ Xor y^k,

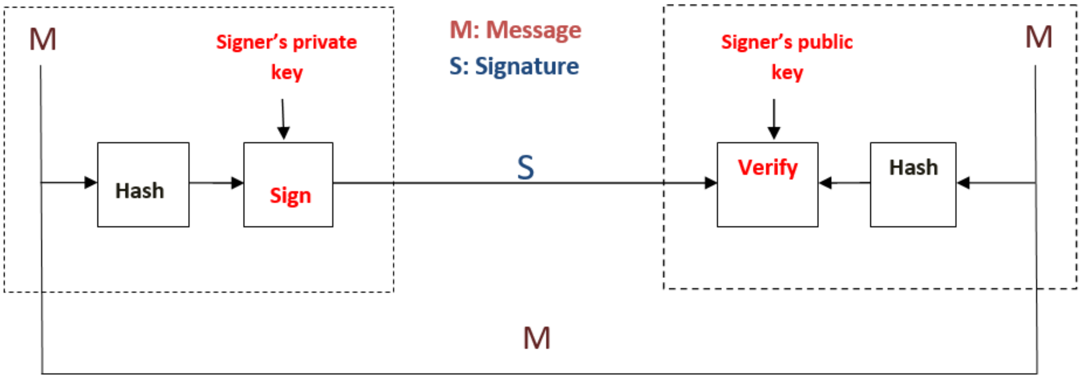
P2 sends **(y_1, y2)** to P1. Upon receiving the ciphertext, P1 computes

m = (y_1^a mod p) **Xor** y_2

3.2.5. ELLIPTIC CURVE CRYPTOGRAPHY (ECC) - ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. It is a public key algorithm that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The security level, which is given by RSA, can be provided even by smaller keys of ECC. For example, the 1024-bit security strength of an RSA could be offered by 163 bit security strength of ECC. Other than this, ECC is particularly well suited for wireless communications, like mobile phones and smart cards. EC point of multiplication operation is found to be computationally more efficient than RSA exponentiation

3.2.6. DIGITAL SIGNATURE STANDARD (DSS) - It is an FIPS (Federal Information Processing Standard) for digital signatures proposed by NIST in 1991. A digital signature is an electronic equivalent of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). A digital signature algorithm includes a signature generation process and a signature verification process. The private key is used in the signature generation process and the public key is used in the signature verification process. For both the signature generation and verification processes, the message (i.e., the signed data) is converted to a fixed-length representation of the message by means of an approved hash function. Both the original message and the digital signature are made available to a verifier who can verify the signature with the signer's public key.

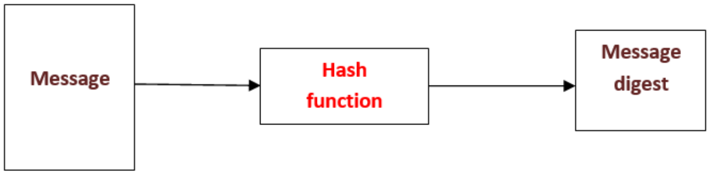
FIG. 1: DIGITAL SIGNATURE PROCESS



4. MESSAGE INTEGRITY AND AUTHENTICATION

4.1. CRYPTOGRAPHIC HASH FUNCTIONS – A Cryptographic Hash Function is an algorithm that creates a compressed image of the message called a message digest that can be used to check the integrity of the message.

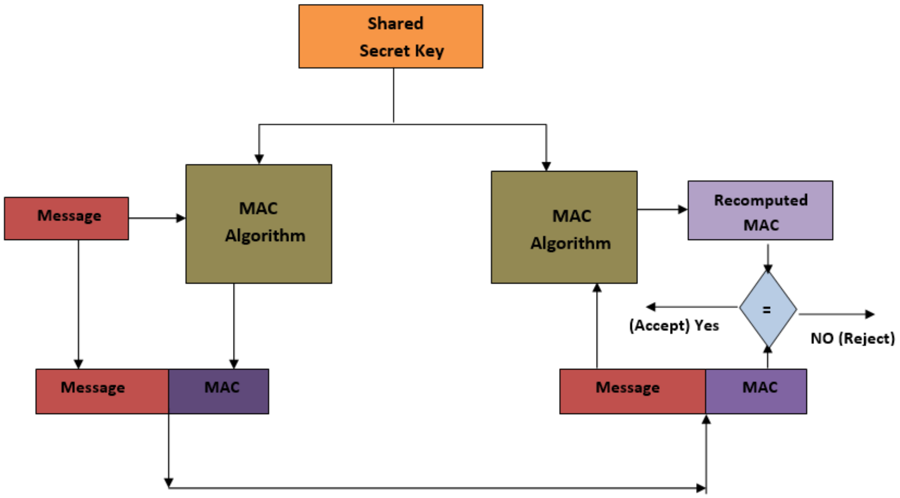
FIG. 2: MESSAGE DIGEST CREATED FROM MESSAGE



To check the integrity of the message, it is passed through **Cryptographic Hash Function**. The new digest is compared with the previous one. If both are same, that means the original message has not changed.

4.1.1. MESSAGE AUTHENTICATION CODE (MAC) - A message digest guarantees only integrity of the message. However, it does not authenticate the sender of the message. A message authentication code provides integrity as well as authentication of the message. The difference between a message digest and MAC is that the latter involves a secret between the communicating entities. A MAC is created by the passing the message, concatenated with the secret key through the hash function.

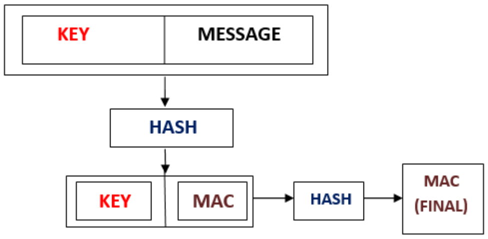
FIG. 3: MAC PROCESS



The receiver separates the message from MAC and creates a new MAC from the concatenation of the message and secret key. Then the newly computed MAC is compared with the MAC received along with the message. If the two MAC's matches, then the message is authentic and has not been modified by any intruder. The intruder cannot forge a new message to replace it since he doesn't possess the secret key between the communicating entities.

4.1.2. NESTED MAC- To improve the security of MAC nested MAC's were designed in which hashing is done in two steps. First the message, concatenated with the secret key is hashed to create message digest. The intermediate digest is again concatenated with the key and hashed to create the final digest.

FIG. 4: NESTED MAC



4.1.3. HASHED MESSAGE AUTHENTICATION CODE (HMAC)- NIST has issued a standard for nested MAC (FIPS 198) which is known as HMAC. It is more complex than nested MAC.

1. The message is divided into N blocks, each of b bits.
2. The secret key is left padded with 0's to create a b-bit key.
3. The key after padding is Ex-ored with a constant called i-pad (input pad) to create a bit block. The value of i-pad is b/8th repetition of the sequence 00110110.
4. The resulting block is prepended to the N-block message which results in N+ 1 blocks.
5. The result of step 4 is hashed to create an n-bit digest (intermediate HMAC).
6. The intermediate HMAC is left padded with zero's to create a b-bit block.
7. Steps 2 and 3 are repeated with a different constant opad (output pad). The value of opad is b/8th repetition of the sequence 01011100.
8. The result of step 7 is prepended to the block of step 6.
9. The result of step 8 is hashed with the same hashing algorithm to create the final n-bit HMAC.

4.1.4. CIPHER BASED MESSAGE AUTHENTICATION CODE (CMAC) - It is also a NIST defined standard (FIPS 113) called Data Authentication Algorithm, or CMAC. It is a block cipher-based message authentication code algorithm. It may be used to provide assurance of the authenticity and, hence, the integrity of binary data. This mode of operation fixes security deficiencies of CBC-MAC (CBC-MAC is secure only for fixed-length messages). To generate an ℓ-bit CMAC tag (t) of a message (m) using a b-bit block cipher (E) and a secret key (k), one first generates two b-bit sub-keys (k_1 and k_2) using the following algorithm:

Let $\ll$ denote the standard left-shift operator and $\oplus$ denote exclusive or:

1. Calculate a temporary value $k_0 = Ek$ (0)
2. If msb (k_0) = 0, then $k_1 = k_0 \ll 1$, else $k_1 = (k_0 \ll 1) \oplus C$; where C is a certain constant that depends only on b. (Specifically, C is the non-leading coefficients of the lexicographically first irreducible degree-b binary polynomial with the minimal number of ones.
3. If msb (k_1) = 0, then $k_2 = k_1 \ll 1$, else $k_2 = (k_1 \ll 1) \oplus C$.
4. Return keys (k_1, k_2) for the MAC generation process.

The CMAC tag generation process is as follows:

1. Divide message into b-bit blocks $m = m_1 \| ... \| m_{n-1} \| m_n$ where $m_1,..., m_{n-1}$ are complete blocks. (The empty message is treated as 1 incomplete block.)
2. If m_n is a complete block then $m_n' = k_1 \oplus m_n$ else $m_n' = k_2 \oplus (m_n\| 10...0_2)$.
3. Let $c_0 = 00...0_2$.
4. For i = 1,....., n-1, calculate $c_i = E_k(c_{i-1} \oplus m_i)$.
5. $C_n = E_k(c_{n-1} \oplus m_n')$
6. Output $t = \text{msb}_\ell(c_n)$.

The verification process is as follows:

1. Use the above algorithm to generate the tag.
2. Check that the generated tag is equal to the received tag.

5. OTHER NETWORK SECURITY TECHNOLOGIES

5.1. FIREWALL- a firewall is a system or group of systems that enforces an access control policy between two networks. It can consist of hardware and software, or even several components working together. It is a single point of defence between two networks. The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks.

There are many ways to implement firewalls on today's corporate networks. Usually they can be thought of as two mechanisms: one that permits traffic and one that exists to block traffic. Firewalls are designed to protect your network from attacks originating from another network. An effective firewall will allow authorized access only to the protected network and deny access to those who don't have it. Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than those against the email service. Other firewalls provide less strict protections and block services that are known to be problems. A more effective firewall will allow users on the protected network to communicate freely with the outside world, as this is the reason a company connects its LAN to the Internet. If a company wants to monitor the types and amounts of traffic that are directed at its network, a firewall can effectively supply this information to the system administrator.

TYPES OF FIREWALL

i. **PACKET FILTER FIREWALL**- They are the simplest firewalls. Packet filters work by dropping packets based on their source or destination addresses or service (i.e., port number). In general, no context is kept; decisions are made only from the contents of the current packet. Depending on the type of router, filtering may be done at input time, at output time, or both. The administrator makes a list of the acceptable machines and services and a stop List of unacceptable machines or services. It is easy to permit or deny access at the host or network level with a packet filter.

ii. **CIRCUIT GATEWAYS** -Circuit gateways operate at the network transport layer. Again, connections are authorized based on addresses. Like filtering gateways, they (usually) cannot look at the data traffic flowing between one network and another, but they do prevent direct connections between one network and another.

iii. **APPLICATION GATEWAYS**- Application gateways or proxy-based firewalls operate at the application level and can examine information at the application data level. They can make their decisions based on application data, such as commands passed to FTP, or a URL passed to HTTP.

5.2. INTRUSION DETECTION SYSTEM (IDS) – An intrusion is an act where someone tries to access a system or information which they are not authorised to. An Intrusion Detection System (IDS) is a software application that monitors the network or system activities for malicious activities and unauthorized access to devices. IDSs collect information from a computer or a computer network in order to detect attacks and misuses of the system. Many IDSs only analyze the attacks and some of them try stopping the attack at the time of the intrusion. Three types of data are used by IDSs. These are network traffic data, system level test data and system status files.

Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them. It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusion detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyse the security problems so that they are not repeated.

6. CONCLUSION AND FUTURE PROSPECTS

As we are heading towards a digital information era, bulk of important and confidential data is produced and transferred everyday across the globe over the internet that makes it vulnerable to numerous types of attacks and threats. So network security has become a major concern for every organisation, be it corporate, defence, government, banking, education etc.

This paper highlighted various Cryptography techniques developed to provide network security. Developing efficient cryptography algorithms which are difficult to break and immune to newer attacks and threats designed every day is the biggest challenge.

With the advent of the internet, network security has become a demanding and challenging area and there is a need to promote more and more research activities in the field of network security.

REFERENCES

1. 07_Common Symmetric Algorithms and Hash Algorithms. (n.d.). Retrieved from https://www.coursehero.com/file/p4rbvhd/Symmetric-Encryption-Symmetric-encryption-is-the-oldest-and-best-known/
2. A. K., & Singh, H. (2014). Network Security: a literature review. *International Journal of Emerging Research in Management &Technology, 3*(10), 32-39. Retrieved May 18, 2017, from https://www.ermt.net/docs/papers/Volume_3/10_October2014/V3N10-116.pdf.
3. Advanced Encryption Standard. (n.d.). Retrieved May 11, 2017, from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
4. Amara, M., & Siad, A. (2011, June 27). Elliptic Curve Cryptography and its applications. Retrieved May 14, 2017, from http://ieeexplore.ieee.org/abstract/document/5931464/
5. Art of cryptography. (2012, November 18). Retrieved May 14, 2017, from http://carbonhacking.blogspot.in/2012/11/art-of-cryptography.html (n.d.). Retrieved from http://www.innovativeresearchpublication.com/documents/goa/paper%2063.pdf
6. Aydin, M. A., Zaim, A. H., & Ceylan, K. G. (2009). A hybrid intrusion detection system design for computer network security. *Elsevier, 35*, 517-526. Retrieved May 15, 2017, from http://eportfolio.lib.ksu.edu.tw/user/G/9/G980Q001/repository/sdarticle.pdf
7. Bellovin, S. M., & Cheswick, W. R. (1994, September). Network Firewalls. *IEEE Communications magazine*, 50-57.
8. Benatar, M. (2002, June 7). Secret Key Cryptography. Retrieved May 12, 2017, from http://www.informit.com/articles/article.aspx?p=27132&seqNum=6
9. Bradford, C. (2017, July 31). 5 Common Encryption Algorithms and the Unbreakables of the Future. Retrieved May 13, 2017, from https://www.storagecraft.com/blog/5-common-encryption-algorithms/
10. Cryptographic MAC based message authentication. (2011, May 2). Retrieved May 14, 2017, from https://commons.wikimedia.org/wiki/File:Cryptographic_MAC_based_message_authentication.png
11. Cryptography. (n.d.). Retrieved May 11, 2017, from https://en.wikipedia.org/wiki/Cryptography
12. Data Encryption Standard (DES). (n.d.). Retrieved May 11, 2017, from http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
13. Elliptic curve cryptography. (n.d.). Retrieved May 14, 2017, from https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
14. F. A. (n.d.). Firewalls and Internet Security - The Internet Protocol. Retrieved May 16, 2017, from http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html
15. Forouzan, B. A. (2007). *CRYPTOGRAPHY AND NETWORK SECURITY*. NEW DELHI: TATA McGRAW-HILL PUBLISHING COMPANY LIMITED.
16. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
17. Internet Security Policy - Internet Firewall Policy. (n.d.). Retrieved from http://www.windowsecurity.com/whitepapers/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Internet_Firewall_Policy.html
18. Kerry, C. F., & Gallagher, P. D. (n.d.). Digital Signature Standard. Retrieved May 11, 2017, from https://oag.ca.gov/sites/all/files/agweb/pdfs/erds1/fips_pub_07_2013.pdf
19. One key MAC. (n.d.). Retrieved May 14, 2017, from https://en.wikipedia.org/wiki/One-key_MAC
20. Secret-Key algorithms. (n.d.). Retrieved May 12, 2017, from http://www.wowarea.com/english/help/secalg.htm
21. Vacca, J. R., & Ellis, S. R. (2007, September 2). Firewalls: What Are They? Retrieved May 15, 2017, from http://www.sciencedirect.com/science/article/pii/B9781555582975500037
22. Verma, S. K., & Ojha, D. D. (january 2012). A Discussion on Elliptic Curve Cryptography and Its Applications. *International Journal of Computer Science Issues, 9*(1), 74-77. Retrieved from http://www.ijcsi.org/papers/IJCSI-9-1-1-74-77.pdf
23. What is Diffie-Hellman Key Exchange/Sharing/Establishment. (n.d.). Retrieved from http://www.omnisecu.com/tcpip/what-is-diffie-hellman-key-exchange.php
24. "What is the ElGamal Cryptosystem?" *Http://x5.net/faqs/crypto/q29.html*. N.p., n.d. Web**.**

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 to supply 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 you have 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 to 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

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

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