INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed Refereed 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.

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

Registered & Listed at: Index Copernicus Publishers Panel, Poland

Circulated all over the world & Google has verified that scholars of more than 1388 Cities in 138 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

www.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We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, 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 addresses: infoijrcm@gmail.com or info@ijrcm.org.in.

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 mention the 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, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

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

WEBSITE

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

SECURE KEY EXCHANGE WITH RANDOM CHALLENGE RESPONSES IN CLOUD

BINU V. P
RESEARCH SCHOLAR
DEPARTMENT OF COMPUTER APPLICATIONS
COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY
COCHIN

DR. SREEKUMAR A
ASSOCIATE PROFESSOR
DEPARTMENT OF COMPUTER APPLICATIONS
COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY
COCHIN

ABSTRACT

With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data. We establish a secure challenge response protocol for sharing a secret key in the cloud environment where users want to access a document encrypted by an owner without the intervention of the service provider. In order to do this, user need to get the key from the document owner in a secure way. Any trusted users in the environment can obtain the key using random challenges. The challenge response protocol uses quadratic residuosity techniques from number theory. The proposed scheme does not use any encryption techniques so the computation requirement is greatly reduced and hence it can also be used efficiently in devices with limited computation power.

KEYWORDS
Key exchange; Random Challenge; Secure Cloud; Qudratic Residuosity.

INTRODUCTION

Cloud computing [10], as an emerging computing paradigm, enables users to remotely store their data in a cloud, so as to enjoy services on-demand. Migrating data from the user side to the cloud offers great convenience to users, since they can access data in the cloud anytime and anywhere, using any device, without caring about the capital investment to deploy the hardware infrastructures. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and the flexibility to scale (or shrink) investments on-demand, by using cloud-based services to manage projects, enterprise-wide contacts and schedules, and the like.

However, allowing a Cloud Service Provider (CSP), operated for making a profit, to take care of confidential corporate data, raises underlying security and privacy issues. For instance, an untrustworthy CSP may sell the confidential information about an enterprise to its closest business competitors for making a profit. Therefore, a natural way to keep sensitive data confidential against an untrusted CSP is to store only the encrypted data in the cloud.

But there are application scenarios where users want to access the data encrypted and store by other users (owners) in a corporate environment. This raises a situation where a secret key used to encrypt a document must be shared among the users for mutually sharing documents. Consider the following application scenario [9] Company A pays a CSP for sharing corporate data in cloud servers. Suppose the sales department (SD), the research and development department (RDD), and the finance department (FD) are collaborating in Project X. The SD manager wants to store an encrypted user requirement analysis (URA) in the cloud, so that only the personnel that have secret key can access the document as shown in Fig. 1. The CSP must maintain proper authentication mechanism and access control policies for granting access but the secret key must be shared directly to the user by the owner.

Diffie-Hellman Key exchange was used to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. But this technique cannot be used to agree upon a specific key by the sender and the receiver.

The proposed scheme can be used to establish a specific shared secret key between sender and the receiver with the help of random challenges.

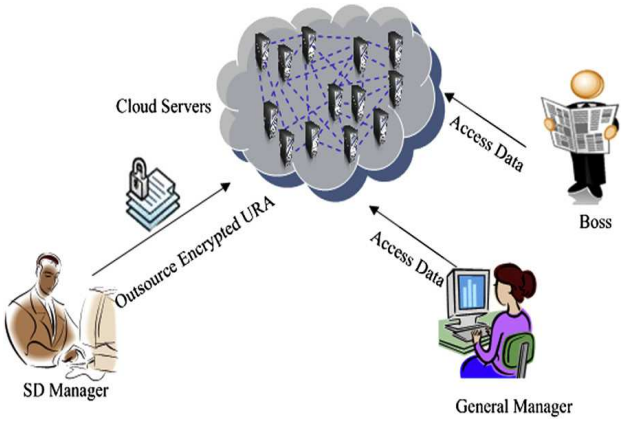

FIGURE 1: THE SAMPLE SCENARIO

SYSTEM MODEL

We assume that the system is composed of the following parties: the CSP, the trusted third party (TTP), enterprise users, end users, and internal trusted parties (ITPs). The first two parties can be easily understood: the CSP operates a large number of interconnected cloud servers with abundant storage capacity and computation power to provide high quality services and the TTP is responsible for generating keys for the CSP and enterprise users. Company A that pays for

sharing corporate data in cloud servers is an enterprise user, all personnel in the company, who share data in cloud servers are end users, and a department in the company that delegates keys inside the company is the ITP.

There are two main attacks under such a circumstance, i.e., external attacks initiated by unauthorized outsiders, and internal attacks initiated by an honest but curious CSP ,as well as malicious end users. Since data is stored with the encrypted form in the cloud and communication channels between users and cloud are assumed to be secured under existing security protocols such as SSL, we only consider the internal attacks. The honest but curious CSP will always correctly execute a given protocol, but may try to learn some additional information about the stored data. The malicious end user wants to access the data that he is ineligible to decrypt. We assume that the CSP will not collude with the end users, since the CSP is considered to be honest but curious.

KEY EXCHANGE PROBLEM

Alice and Bob have to share a secret SA own by Alice. Let SA is the password of a file which Bob want to access or it may be encryption key. The question is how Alice can exchange this key to Bob without a trusted third party.

Several key establishment protocols and key management techniques [5] are used in secure communication between the parties. RSA [6] and Diffie-Hellman [7] are the most widely used techniques. Both use public key techniques to allow the exchange of a private encryption key.

Both RSA and Diffie-Hellman are public key encryption algorithms strong enough for commercial purposes. The minimum recommended key length for encryption systems is 128 bits, and both exceed that with their 1,024-bit keys. The nature of the Diffie-Hellman key exchange, however, makes it susceptible to man-in-the-middle (MITM) attacks, since it doesn't authenticate either party involved in the exchange. The MITM maneuver can also create a key pair and spoof messages between the two parties, who think they're both communicating with each other. Mutually authenticating both parties can defeat attempts at MITM attacks.

Diffie-Hellman scheme can be used to set up a shared secret key but the two parties engaged in the protocol cannot set up a specified key as they wish. So this technique cannot be used to agree upon a specific key by the sender and the receiver.

The key exchange can also be done with RSA algorithm but the computational complexity is more and also it needs a trusted third party for the distribution of private and public keys. Techniques are also implemented to exchange secrets by oblivious transfer by M. O. Rabin [8].

The proposed scheme does not use any encryption techniques so it can be used in devices with less computational power. It uses only simple arithmetic operations in the field.

PRELIMINARIES

In this section we give some mathematical techniques from number-theory [3] and state the Quadratic Residuosity (QR) problem [4], which is the principal technique used here. The quadratic residuosity was first used in the cryptographic setting by Gold wasser and Micali [2]. Then it has found many applications in cryptography. It is used by Eyal Kushilvetz and Rafail Ostrovsky for computationally-Private Information Retrieval [1]. We shall use in this work the intractability of the Quadratic Residuosity problem.

Quadratic Residues

Let us consider the quadratic congruence of the form

$$x^2 \equiv y \pmod{p}$$

Where p is an odd prime and $y \not\equiv 0 \pmod{p}$. If the congruence has a solution we say that y is a quadratic residue (QR) $mod\ p$ else quadratic non residue (QNR) $mod\ p$.

The basic problem that dominates the theory of quadratic residue is, given p, determine which y are quadratic residues $mod\ p$ and which y are quadratic non residues $mod\ p$.

If N is a positive odd integer with prime factorization.

$$N = \prod_{i=1}^{r} p_i^{ai}$$

The Jacobi symbol $(y|N)$ is defined for all integers y by the equation

$$(y|N) = \prod_{i=1}^{r} (y|p_i)^{ai}$$

Where $(y|p_i)$ is the Legendre symbol.

If the congruence $x^2 \equiv y \pmod{N}$ has a solution then $(y|p_i) = 1$ for each prime p_i and hence $(y|N) = 1$. However the converse is not true since $(y|N)$ can be 1 if an even number of factors is -1. So it will be difficult to distinguish the residues and non residues. The problem is considered hardest when N is a product of two distinct primes of equal length. If the factorization of N is known it can be done easily. The real complexities lie in the prime factorization of large N.

PROPOSED SCHEME

Assumptions

The key is assumed to be a binary string of specified length. The scheme provides better security if the key bits can be represented as square matrix of a particular size.

Let $b1b2b3 \ldots bn$ be the bits of the key to be exchanged between the sender and the receiver. K is an mxn matrix representing the key bits.(make m and n equal for better security).The following figure(Fig.2) shows the organization of 64 bit key .

b1	b2	b3	b4	b5	b6	b7	b8
b9	b10	b11	b12	b13	b14	b15	b16
b17	b18	b19	b20	b21	b22	b23	b24
b25	b26	b27	b28	b29	b30	b31	b32
b33	b34	b35	b36	b37	b38	b39	b40
b41	b42	b43	b44	b45	b46	b47	b48
b49	b50	b51	b52	b53	b54	b55	b56
b57	b58	b59	b60	b61	b62	b63	b64

FIGURE 2: KEY MATRIX K ($8X8$)

The owner wants to share a secret key of a particular encrypted document with the user. The owner and the user must be authenticated by the CSP to access the resources. The protocol uses a challenge response technique and at the end of the protocol the receiver will be able to reconstruct the key from K.

Key Exchange with Random Challenge Protocol

Now we are ready to define key exchange algorithm with challenge response protocol.

Let N be a natural number define

$Z_N^* = \{x \mid 1 \leq x < N, \gcd(N, x) = 1\}$

$Z_N^+ = \{y \in Z_N^*, (y|N) = 1\}$

The user selects two random *k/2* bit prime numbers and the product N is a k bit random number. The user sends N to the owner but keeps its factorization secret.

The user picks uniformly at random *n* numbers which are not perfect squares, $y_1, y_2, y_3, \ldots, y_n \in Z_N^+$, such that y_c is a QNR and y_j, for $j \neq c$, is a QR. Here each number corresponds to one column of the matrix *K*. He sends these *n* numbers to the owner (total of $n * k$ bits).

The owner computes for every row *r* a number $Z_r \in Z_N^*$,as follows: It first computes (in Z_N^*)

$$Kr,j = \begin{cases} y_j^2 & if\ Kr,j = 0 \\ y_j & if\ Kr,j = 1 \end{cases}$$

Where $1 <= j <= n$, then it computes

$$Z_r = \prod_{i=1}^{r} Kr,j$$

The observation here is that if $j \neq c$ then Kr,j is always a QR, while if $j = c$ then Kr,j is QR iff $Kr,j = 0$ and it is QNR otherwise. Therefore Z_r is a QR iff $Kr,j = 0$

The set of Z_r computed for each row $1 <= r <= m$ is send to the user by the owner (total of $m * k$ bits).

With these Z_r , the user will be able to retrieve the column *c* of K by computing and checking each of the received Z_r for QR or QNR.

The above procedure from can be repeated for different values of *c* and obtain the other columns also.

The challenge response protocol ends when the user retrieves *K* after n rounds.

The selection of QR and QNR can be done efficiently using the following method.

For QR, choose a random number y which is in Z_N^*, square it and find $mod\ N$.

For QNR choose a random number *y*

if $(y|p) = -1$ *and* $(y|q) = -1$*, then y is a QNR.*

If $(y|p) = -1$ *and* $(y|q) = 1$*, if for another x if* $(x|p) = 1$ *and* $(x|q) = -1$*, then we can combine x and y to efficiently compute a QNR,* $(xy|N)$.

If $(y|p) = 1$ *and* $(y|q) = 1$*, neglect the y and try the next random number.*

The QNR can be computed efficiently if p (or q) in the form, $4n + 3$. In this case take any random number r and find $p - (r^2\ mod\ p)$ which will be a QNR.

Once a QNR is obtained, we can use it to find another QNR and then use it in the next challenge by computing $(r^2 y|N)$, where y is the previously obtained QNR and r is a random number.

Do not choose *c* sequentially. The value of *c* must be chosen randomly so that the adversary does not have any idea which column the user is retrieving. Also different N must be chosen for each challenge. The challenge and response will have the same size because K is a square matrix. So the adversary cannot distinguish between challenge and response.

We can also consider the operations in an alternate way by retrieving the rows of key matrix where the key bits organized in each column sequentially.

Communication complexity

The communication in this scheme consists of $m + n + 1 - k$ bit numbers $(N, y_1, y_2, y_3, \ldots, y_n, Z_1, Z_2, \ldots Z_m)$.

Pick $m = n = \sqrt{K_n}$ and the communication complexity in one challenge is $\left(2\sqrt{K_n} + 1\right) * k$ bits, where K_n is the number of bits in the key. The major factor deciding the security and communication complexity is k, which depends on the size of N. The number of rounds in the protocol is decided by n, which depends on the size of the key to be shared.

CONCLUSION AND FUTURE DIRECTIONS

We have described a new technique for exchanging a secret key using random challenge responses. The protocol can be used to exchange a specific key unlike setting up a random key between the sender and the receiver. This scheme can also be used to share different keys with different users in an efficient way. An efficient authentication scheme can also be implemented where unauthorized users can be easily identified without using an encryption technique, which is required in the conventional random challenge response technique.

In the cloud-computing environment, users may access data anytime and anywhere using any device. When a user wants to access data using a thin client with limited bandwidth, CPU, and memory capabilities, we need to develop algorithms with low communication and computational costs. An efficient delegation mechanism and revocation scheme must also be incorporated with this scheme for the key management in the enterprise scenario.

ACKNOWLEDGEMENT

The present paper is presented in NCETCT 2012, National Conference on 'Emerging Trends in Computing Technology', organised by Department of Computer Science & Engineering, Archana College of Engineering, Palamel, in collaboration of IJRCM.

REFERENCES

1. "Introduction to Cloud Computing," available at http://www.techno-pulse.com/2010/11/download-intro-cloud-computing-pdf.html.
2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone,"Hand Book of Applied Cryptography," CRC Press ISBN: 0-8493-8523-7, October 1996.
3. Guojun Wanga, Qin Liu a,b, Jie Wub, Minyi Guo, " Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," computers and Security, Elsevier,30(2011),320-331.
4. K.McCurely "Odds and Ends from Cryptology and Computational number theory in Cryptography and Computational Number Theory," AMS proceedings of Sumposia in Applied Mathematics, Vol 42, pp. 145-166,1990.
5. Kushilevitz and R. Ostrovsky, "Replication Is Not Needed: Single Database, Computationally-Priavte Information Retrieval," in Proc. Of the 38th FOCS, 1997, pp. 364-373
6. M. O. Rabin. "How to exchange secrets by oblivious transfer." Technical Report TR-81, AikenComputation Laboratory, Harvard University, 1981.
7. Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21 (2): 120–126. doi:10.1145/359340.359342.
8. S.Gold wasser and S.Micali, "Probabilistic Encryption," Journal of Computer and System Sciences 28,270-299,1984.
9. Tom M Apostol, Introduction to Analytic Number Theory, Springer International Student Edition.
10. W. Diffie and M. E. Hellman," New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644–654.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, Internation]al Journal of Research in Commerce, IT and 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-mails i.e. **infoijrcm@gmail.com** or **info@ijrcm.org.in** 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 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