ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

AN EMPIRICAL ANALYSIS AND SIMULATION OF A COLLISION AVOIDANCE ALGORITHM FOR SECURE DATA EXCHANGE AND NON REDUNDANT PACKET TRANSMISSION

Harpreet Aneja
Research Scholar
Lovely Professional University
Jallandhar, Punjab, India

Abstract
The secure transmission of data in transit relies on both cryptography and authentication − on both the hiding or concealment of the data itself, and on ensuring that the computers at each end are the computers they say they are. In this paper a priority based collision avoidance algorithm for secure data exchange is proposed where the encryption and decryption process uses hash function and authentication is supported via username password. The algorithm provides the unique feature of collision and redundancy avoidance and also supports the priority based response from receiver of data or message. This paper simulates the error free, non redundant and collision free packet transmission in the network channel

Keywords: *Priority, collision, data security, authentication, cryptography.*

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

1 INTRODUCTION

The important security risk is that information can be captured and read during its transmission. How do we protect this information from being read by intruders? The secure transmission of data in transit relies on both cryptography and authentication − on both the hiding or concealment of the data itself, and on ensuring that the computers at each end are the computers they say they are.

Cryptography, to most people, is concerned with keeping communications private. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a key. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. There are several ways of classifying cryptographic algorithms. In general they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use as in [1]. The three types of algorithms are depicted as follows

1) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard (AES).

2) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption. RSA (Rivest, Shamir, Adleman) algorithm is an example.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

3) Hash Functions: Uses a mathematical transformation to Irreversibly "encrypt" information. MD (Message Digest)

In this paper a priority based collision avoidance algorithm for secure data exchange is proposed where the encryption and decryption process uses hash function and authentication is supported via username password. The algorithm provides the unique feature of collision and redundancy avoidance and also supports the priority based response from receiver of data or message. Section II presents the detailed study of hash function. Section III describes the proposed algorithm for secure data exchange. Finally section IV concludes the paper and presents the future work directions.

2. Proposed Algorithm and Data Flow Diagram

In this section a priority based collision avoidance algorithm for secure data exchange is proposed which provides the security to the long message in terms of authentication and confidentiality so that the privacy of data does not breach and not any unauthorized user access the data. This algorithm avoids the collision and storage of repeated data when similar messages repeated over network at times and also provides the facility to receiver for responding according to the priority wise and separately to each sender very efficiently. The functional flow diagram and algorithm steps are described in figure 6 and 7 respectively

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

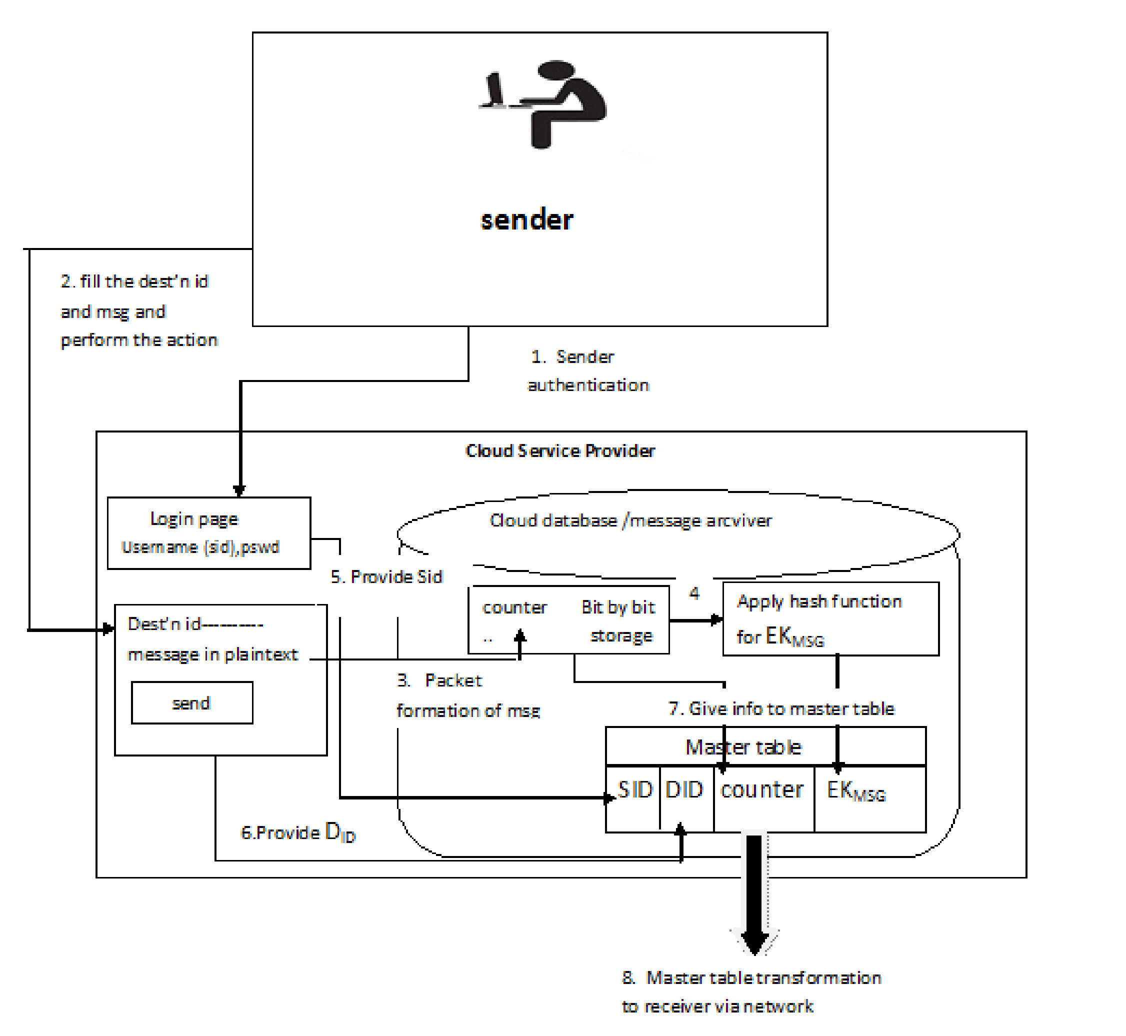


Figure 6. Functional flow diagram for sending encrypted message

Algorithm for sending encrypted message or data

1. Authentication of sender

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

(a) Sender login to cloud server where:

S_{ID} ← Username /* set username of sender as sender id S_{ID}*/

Psw ← password

2. Message Sending: During message sending the following steps are followed by sender:

(a) DID ← Destination user name

/* sender filled the destination Username to which he wants to send the message that is stored as destination id DID*/

(b) Msg ← Plain text /* sender write the message in to the plain text form*/

And send to the receiver

3. Storage of encrypted data in to the cloud server database : After sending the data the message archiver present into the cloud server data base performs the following actions:

(a) Packet formation :

(i) Message archiver receives the message and store it as one by one bit or character in message field of temporary created table

(ii) For each bit counter ←counter+1

(b) Encryption: message archiver perform the hash function on message field

EK_{MSG} ← Hash(message field)

(c) Storage of Master table: message archiver stores the master table into the cloud database which involves following fields:

Master Table ← (S_{ID},D_{ID}, EK_{MSG}, Sequence no/counter)

4. The master table is sent to the receiver via communication link.

5. End of algorithm

The brief description of algorithm is as follow

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

Steps For sending encrypted data

Module 1: Authentication: The sender who wants to send the message firstly login at cloud server for authentication purpose where the sender username is taken as sender id.

Module 2: Message Sending: After login process the CSP requests to the sender to fill the information of destination identity and the message in the form of plain text that he wants to send to the receiver. After providing the required information to CSP the sender performs the action of sending the message by clicking on send button.

Module 3: Packet formation and encryption of message: Before sending the message from sender to receiver the CSP firstly converted the messages into packets and stores it as one by one bit. The counter is also incremented for each character/ bit of message which also deals with the problem of the collision of similar words caused due to the repetition of similar words during the transmission of long message. Cloud service provider also performs the hash function on message for encryption and maintaining their confidentiality.

Module 4: Storage of data as Master Table: The message archiver maintains the master table and stores it into Cloud database that has sender id, destination id, encrypted message and sequence number of whole message in its fields. The master table is then sent to the receiver through any of the network mediums.

The functional flow diagram and algorithm steps are described in figure 8 and 9 respectively.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

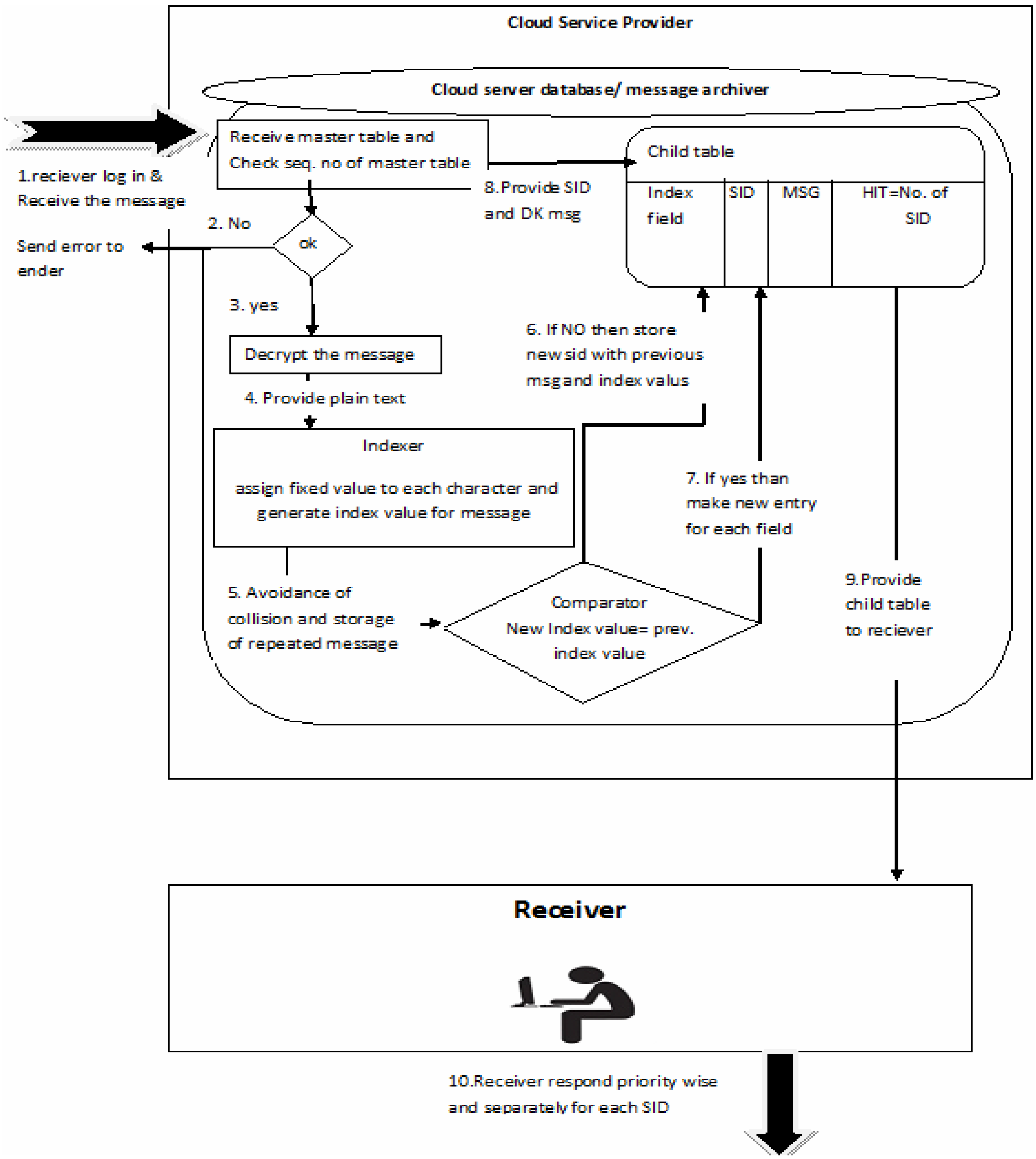


Figure 9. Functional Flow diagram for decrypting the message at receiver side

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

ALGORITHM FOR DECRYPTION OF MESSAGE AND COLLISION AVOIDANCE AT RECEIVER SIDE

1. Receiving and decryption of incoming message
   (a) Receiver side message archiver receives the master table
   (b) Check for sequence number
   If
   sequence number is ok
   Then
   go to step 2
   otherwise
   send an error message to sender
2. Decrypt the message: $DK_{MSG} \leftarrow$ Hash $_{REVERSE}(EK_{MSG})$
3. Creation of child table into the cloud database
   (a) Assigned the fixed value for each character of decrypting message i.e.
   $FX_i \leftarrow i$ /* for each character I the fixed value is FX_i where i= 1 to n */
   (b) Index value $\leftarrow$ ($FX_1 . FX_2 . FX_3 .... FX_4$)
   /* where the index value is equal to the concatenation of fixed values of all characters of decrypted msg */
   (c) Message archiver stores the child table into the cloud database as follow:
   Child table $\leftarrow$ (index value, S_{ID}, DK_{MSG},HITS)
4. Avoidance of collision and storage of repeated message:
   (a) For each incoming message
   If
   Index value $_{new}$=index value $_{prv}$

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

/*where message archiver match the index value for new decrypting message with the index values of previous messages existed in child table */

Then

Store new SID with the previous matched index value and

HIT ← HIT+1

Otherwise

make a new entry for each field of child table

5. Receiver's response to the sender:
   (a) Receiver responds priority wise and separately for each S_{ID} existed into the child table where greater the number of hits represents the higher the priority of message.
6. End of algorithm.

Steps for decrypting the message and avoidance of storage of repeated data at receiver side

Module 1: Check the sequence number for message: receiver side buffer or message archiver receives the Master table and check the sequence number of message. If the sequence number is correct then message archiver decrypts the encrypted message but is the sequence number is not correct then it sends the error message to sender.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

Module 2: creation of child table: The message archiver assigns the fixed value for each character of decrypted message i.e. assign FXi for each i where i=1to n. Message archiver also creates the index value for each message which is the concatenation of the fixed values that are assigned to each character of message and then store the child table into the cloud server that has following fields: index value for each message sender ids, decrypted message and hits that is incremented every time when a sender id is stored in child table.

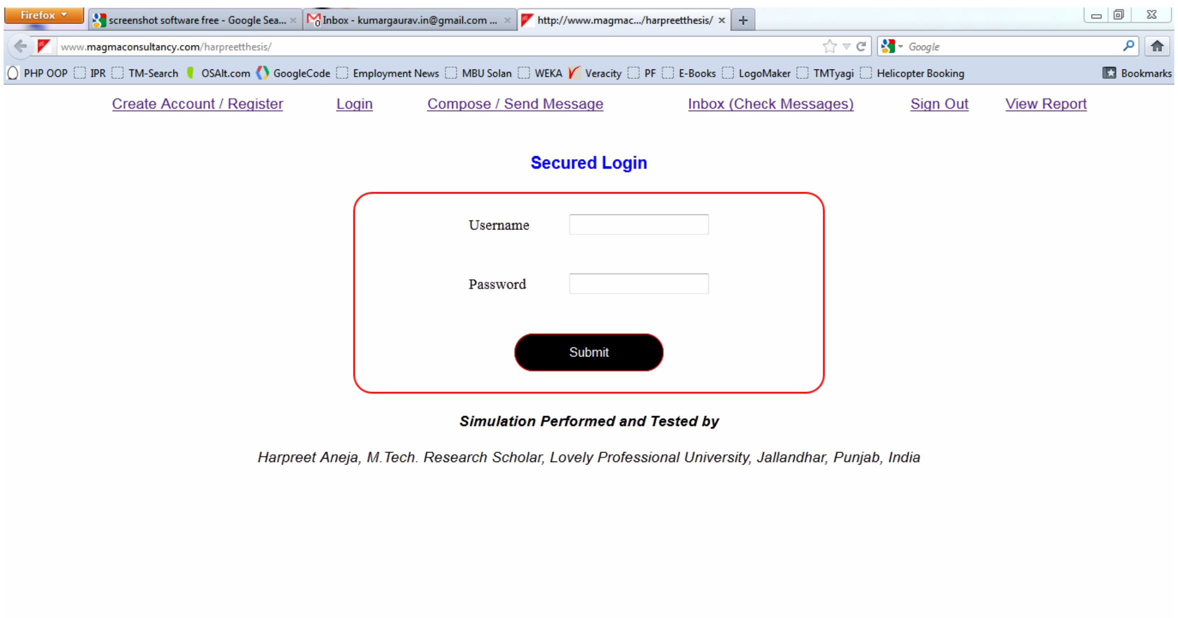
Module 3: Avoidance of collision (loss of information) and storage of repeated messages: for each incoming message , message archiver always checks weather the index value of new arrived message is equal to the index value of any previously existed message. If it matches then only the sender id is stored in child table with the previously existed index value which prevents from the storage of same repeated message again in child table. But if the index values are not matched then message archiver saves a new entry for each field of child table. This technique also prevents from the loss of information due to the collision of same message at times because it always saves the sender id and also increment the number of hits whenever a new message arrived at receiver side.

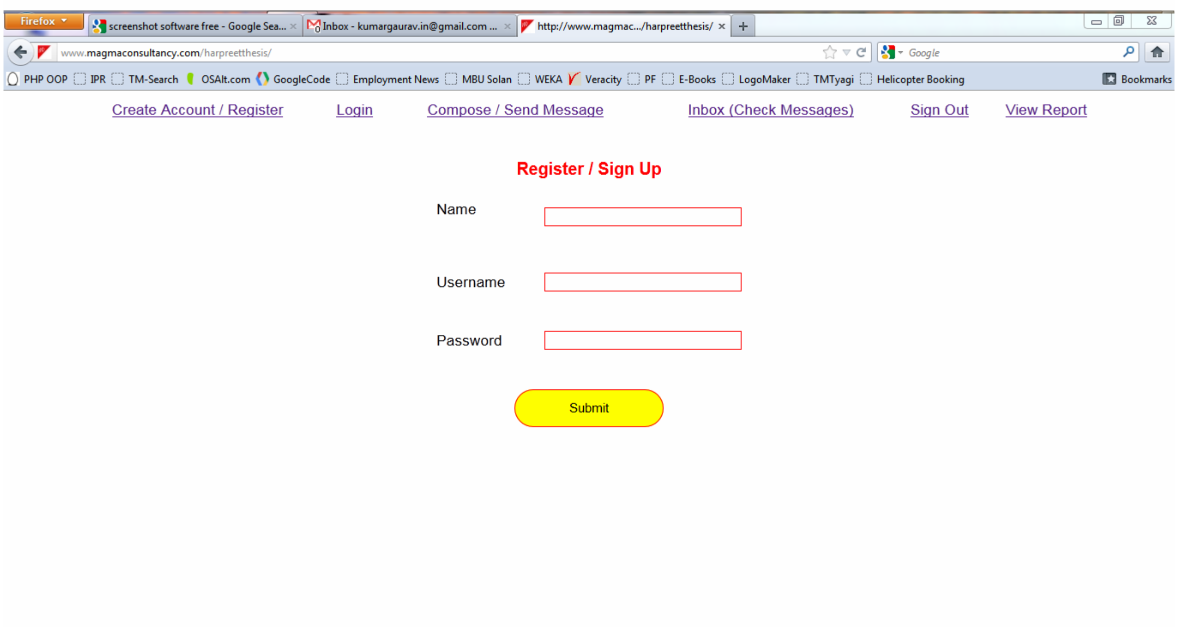
Module 4: Priority wise response of receiver: The child table is sent to the receiver and receiver responds priority wise and separately for each sender id present into the child table. Where greater the number of hits represents highest the priority of message.

SIMULATION RESULTS AND ANALYSIS

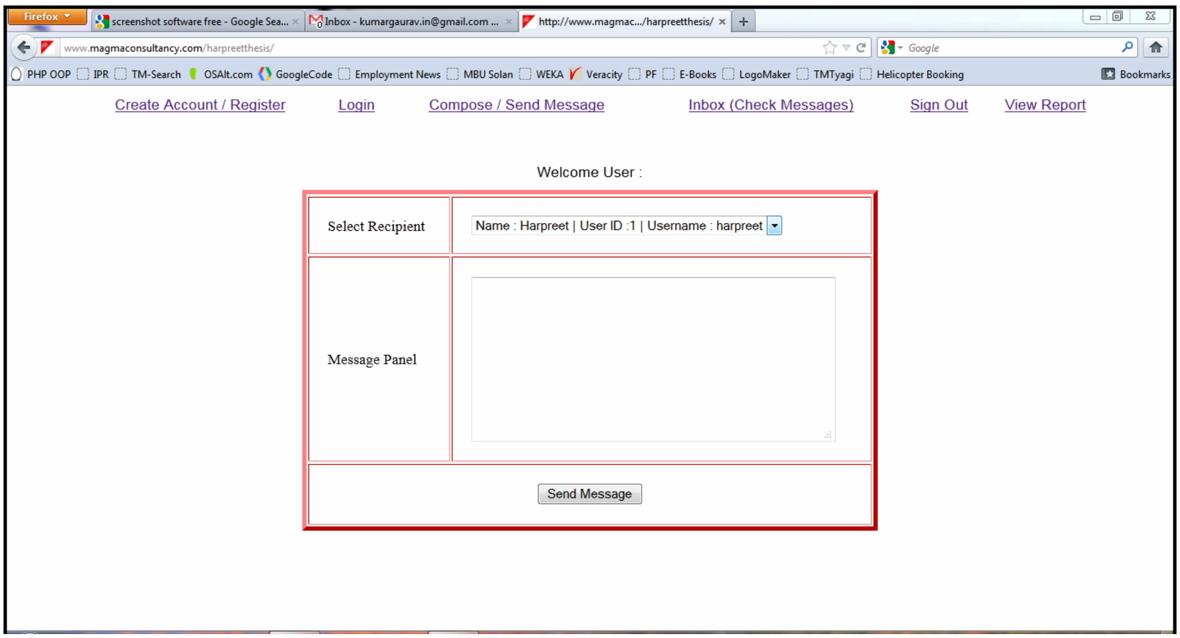
SIMULATION AND RESULTS

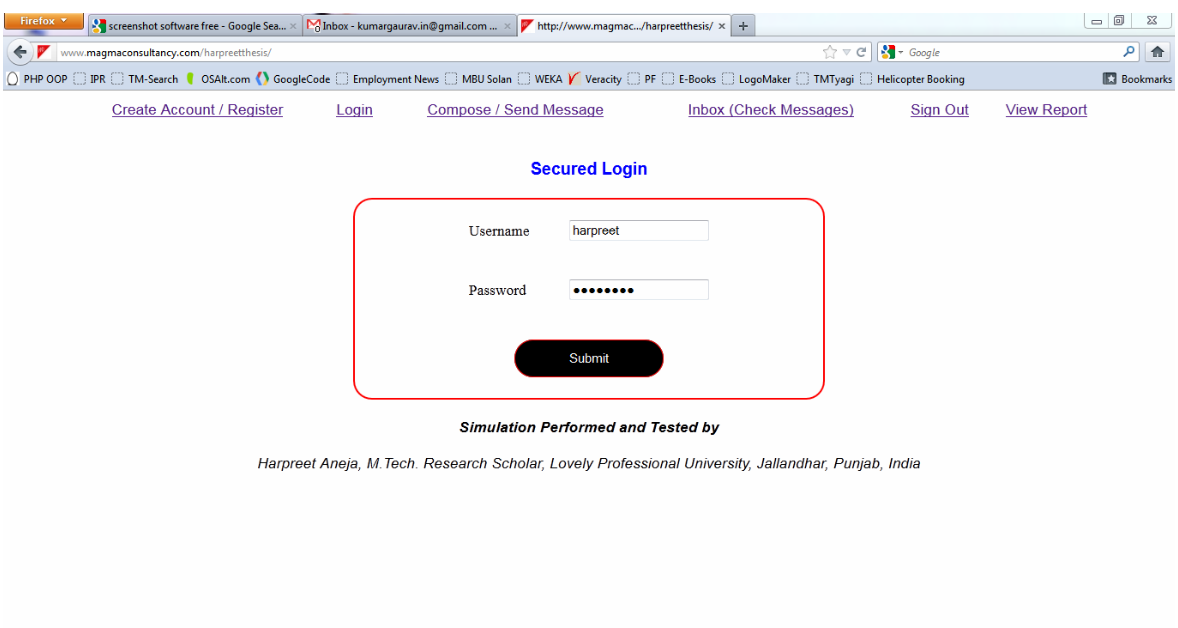
ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012



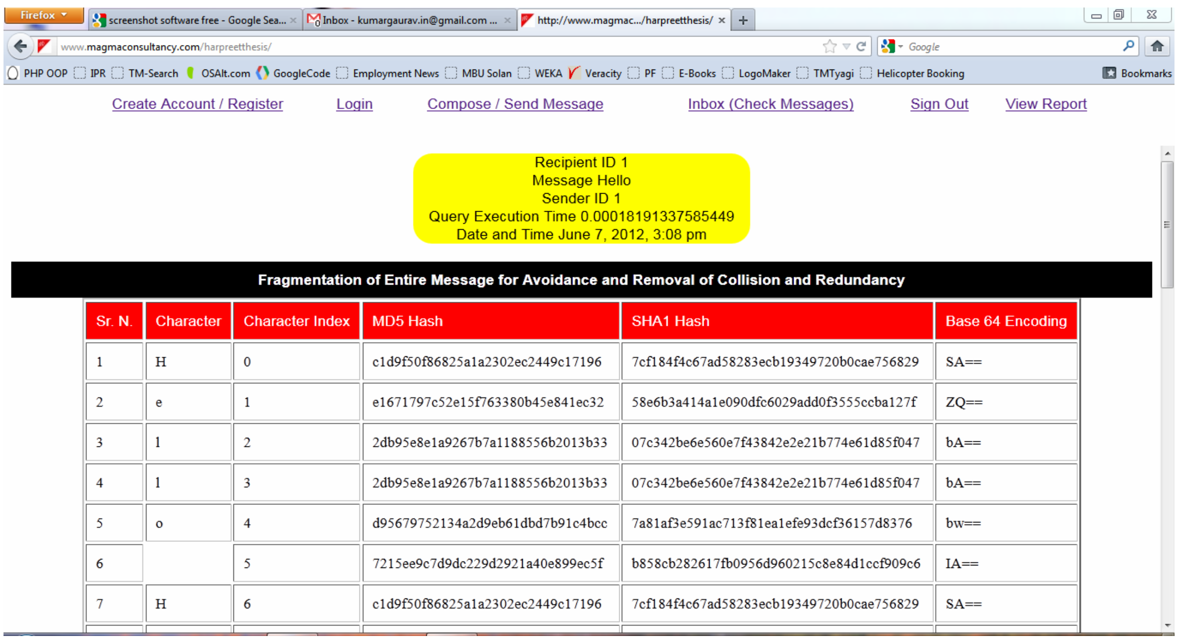


ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012





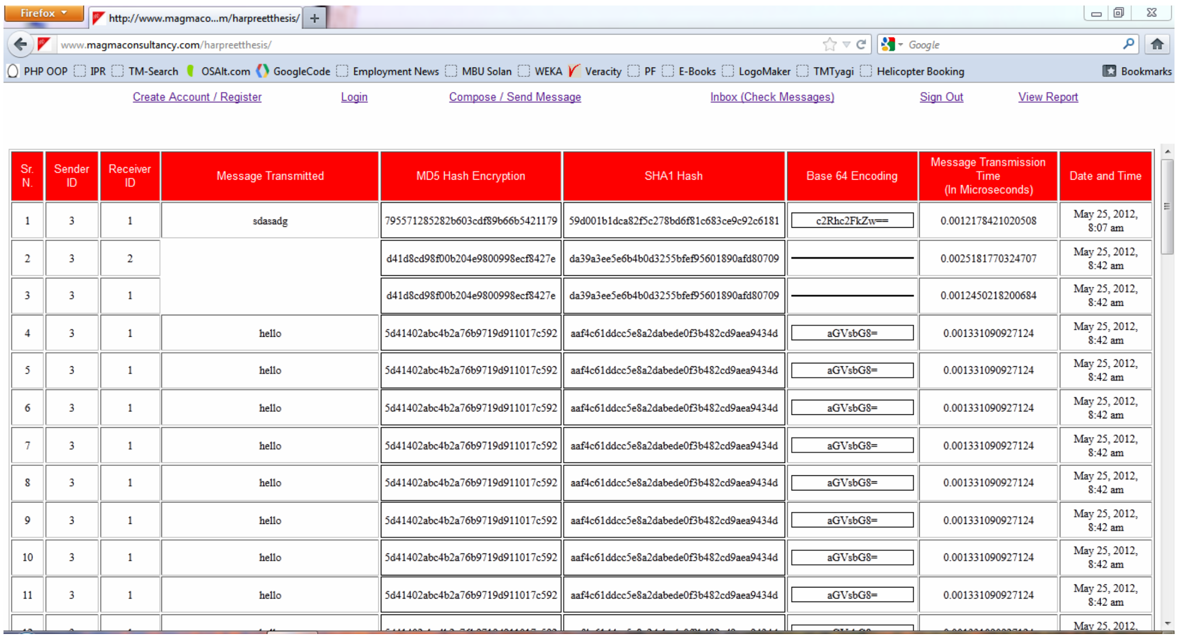
ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012



Fragmentation of Entire Message for Avoidance and Removal of Collision and Redundancy

Sr. N.	Character	Character Index	MD5 Hash	SHA1 Hash	Base 64 Encoding
1	H	0	c1d9f50f86825a1a2302ec2449c17196	7cf184f4c67ad58283ecb19349720b0cae756829	SA==
2	e	1	e1671797c52e15f763380b45e841ec32	58e6b3a414a1e090dfc6029add0f3555ccba127f	ZQ==
3	l	2	2db95e8e1a9267b7a1188556b2013b33	07c342be6e560e7f43842e2e21b774e61d85f047	bA==
4	l	3	2db95e8e1a9267b7a1188556b2013b33	07c342be6e560e7f43842e2e21b774e61d85f047	bA==
5	o	4	d95679752134a2d9eb61dbd7b91c4bcc	7a81af3e591ac713f81ea1efe93dcf36157d8376	bw==
6		5	7215ee9c7d9dc229d2921a40e899ec5f	b858cb282617fb0956d960215c8e84d1ccf909c6	IA==
7	H	6	c1d9f50f86825a1a2302ec2449c17196	7cf184f4c67ad58283ecb19349720b0cae756829	SA==

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012



Sr. N.	Sender ID	Receiver ID	Message Transmitted	MD5 Hash Encryption	SHA1 Hash	Base 64 Encoding	Message Transmission Time (In Microseconds)	Date and Time
1	3	1	sdasadg	795571285282b603cdf89b66b5421179	59d001b1dca82f5c278bd6f81c683ce9c92c6181	c2Rhc2FkZw==	0.0012178421020508	May 25, 2012, 8:07 am
2	3	2		d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.0025181770324707	May 25, 2012, 8:42 am
3	3	1		d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.0012450218200684	May 25, 2012, 8:42 am
4	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
5	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
6	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
7	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
8	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
9	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
10	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
11	3	1	hello	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.001331090927124	May 25, 2012, 8:42 am
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	May 25, 2012,

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

Sr. N.	Sender ID	Sender Name	Message	Date and Time
1	3	Renu	sdasadg	May 25, 2012, 8:07 am
2	3	Renu		May 25, 2012, 8:42 am

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

3	3	Renu	hello	May 25, 2012, 8:42 am
4	3	Renu	hello	May 25, 2012, 8:42 am
5	3	Renu	hello	May 25, 2012, 8:42 am
6	3	Renu	hello	May 25, 2012, 8:42 am
7	3	Renu	hello	May 25, 2012, 8:42 am
8	3	Renu	hello	May 25, 2012, 8:42 am
9	3	Renu	hello	May 25, 2012, 8:42 am

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

10	3	Renu	hello	May 25, 2012, 8:42 am
11	3	Renu	hello	May 25, 2012, 8:42 am
12	3	Renu	dagsdagsdag	May 25, 2012, 9:00 am
13	3	Renu	dagsdagsdag	May 25, 2012, 9:00 am
14	3	Renu	dagsdagsdag	May 25, 2012, 9:00 am
15	3	Renu	dagsdagsdag	May 25, 2012, 9:00 am
16	3	Renu	dagsdagsdag	May 25, 2012, 9:00 am

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

17	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
18	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
19	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
20	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
21	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
22	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am
23	3	Renu	sagdsdag sdga gsda	May 25, 2012, 9:05 am

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

24			sgsdag	May 26, 2012, 12:36 pm
25	3	Renu	hi how r u	May 27, 2012, 6:32 pm
26	2	Pooja	hello how r u	May 27, 2012, 6:39 pm
27	2	Pooja	hello how r u	May 27, 2012, 6:45 pm
28			hello h r u	May 27, 2012, 6:48 pm
29	3	Renu	hello how r u	May 28, 2012, 3:06 pm
30	1	Harpreet	Hello How r u ? Good Afternoon	May 30, 2012, 4:09 pm

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

31	1	Harpreet	Hello	June 7, 2012, 3:08 pm

SIMULATION

Sender ID	Receiver ID	MD5 Hash Encryption	SHA1 Hash	Base 64 Encoding	Message Transmission Time (In Microseconds)
3	1	795571285282b603cdf89b66b5421179	59d001b1dca82f5c278bd6f81c683ce9c92c6181	c2Rhc2FkZw==	0.001217842102050 8
3	2	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.00251817703247 07
3	1	d41d8cd98f00b204e9800998ecf8427e	da39a3ee5e6b4b0d3255bfef95601890afd80709		0.00124502182006 84
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b971	aaf4c61ddcc5e8a2dabede0f3b	aGVsbG8=	0.0013 31090

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

		9d911017c592	482cd9aea9434d		927124
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	5d41402abc4b2a76b9719d911017c592	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	aGVsbG8=	0.0013310909271 24
3	1	ed1034c02f925638493168d476fbd160	bfdb730bf032fa0d7892407f6904c6e35dc8e740	ZGFnc2RhZ3NkYWc=	0.0011861324310303
3	1	ed1034c02f925638493168d476fbd160	bfdb730bf032fa0d7892407f6904c6e35dc8e740	ZGFnc2RhZ3NkYWc=	0.0011861324310303
3	1	ed1034c02f925638493168d476fbd160	bfdb730bf032fa0d7892407f6904c6e35dc8e740	ZGFnc2RhZ3NkYWc=	0.0011861324310303

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

3	1	ed1034c02f925638493168d476fbd160	bfdb730bf032fa0d7892407f6904c6e35dc8e740	ZGFnc2RhZ3NkYWc=	0.00118613243103 03
3	1	ed1034c02f925638493168d476fbd160	bfdb730bf032fa0d7892407f6904c6e35dc8e740	ZGFnc2RhZ3NkYWc=	0.00118613243103 03
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	1	e2a17c6b794245417a8e4dcbeae68ae3	07475db5a0d4139dd9e916d5ac9f5fc503ddc282	c2FnZHNkYWcNCnNkZ2ENCmdzZGE=	0.00167202949523 93
3	2	bb3a85aca632e03955f89c3f0dc3fa9	656d0201d0e1db671c76735e04e3ec49b2f93	YXNkc2RhZw==	0.00193786621093

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

		8	378		75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6 32e03955f8 9c3f0dc3fa9 8	656d0201d0e1 db671c76735e 04e3ec49b2f93 378	YXNkc2RhZw==	0.0019 37866 21093 75
3	2	bb3a85aca6	656d0201d0e1	YXNkc2RhZw==	0.0019

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

		32e03955f89c3f0dc3fa98	db671c76735e04e3ec49b2f93378		378662109375
3	2	bb3a85aca632e03955f89c3f0dc3fa98	656d0201d0e1db671c76735e04e3ec49b2f93378	YXNkc2RhZw==	0.0019378662109375
3	2	bb3a85aca632e03955f89c3f0dc3fa98	656d0201d0e1db671c76735e04e3ec49b2f93378	YXNkc2RhZw==	0.0019378662109375
3	2	bb3a85aca632e03955f89c3f0dc3fa98	656d0201d0e1db671c76735e04e3ec49b2f93378	YXNkc2RhZw==	0.0019378662109375
3	2	bb3a85aca632e03955f89c3f0dc3fa98	656d0201d0e1db671c76735e04e3ec49b2f93378	YXNkc2RhZw==	0.0019378662109375
3	2	bb3a85aca632e03955f89c3f0dc3fa98	656d0201d0e1db671c76735e04e3ec49b2f93378	YXNkc2RhZw==	0.0019378662109375
1	3	8b1a9953c4611296a827abf8c47804d7	f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0	SGVsbG8=	0.0010027885437012
1	4	c92a8c4c9639c8eea645ae900d2d55d0	974d929ed4b5aaab1d1fcf02fea21a48eafc6c48	aGVsbG8gdw==	0.68354010581 97
1	6	26efe432256ef88b79f7559130a982b5	3ebe997f741f14c09be65dff882610f851e3f662	Z2pmZ2oNCmprbGsNCm4sbW5rLA0KamJtYiwNCmtubW4gDQoNCm5odm1iDQpibm5iDQpubWJtYg0Kbm1iLG1uaywNCg==	0.000973939 89562988
	1	59cab9ac39de16f1402912e651b4a6f2	ee13de73a30eecb7cf7d4c161d6a4f4299b1f857	c2dzZGFn	0.92712807655334

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

3	4	163745a94ad2451e897cd2d78723e81b	a792ab28944180df2a4d9bb4686c6ae08592da35	aGVsbG8NCmhvdyBydSA/	0.051976919174194
3	3	26407e224d07f274d9f4953d79a616ec	eae8644396f1224d065b690506de3525c25a7f68	ZGdzYQ0KaGVsbG8=	0.00037693977355957
3	1	b68682e14764463aabec40f464a9c998	00db1a0b08b28e8541a6b4bbd8afab09544c7ad0	aGkgaG93IHIgdQ==	0.00059294700622559
2	1	a71698d590eb6791392f770a45b51073	d4d1a60f8d365a55c8a3abf4065c09ec6409def0	aGVsbG8gaG93IHIgdQ==	0.00052881240844727
2	1	a71698d590eb6791392f770a45b51073	d4d1a60f8d365a55c8a3abf4065c09ec6409def0	aGVsbG8gaG93IHIgdQ==	0.00024580955505371
	1	08f50adbe775ce25c98176453d2c78e3	1b62a81b7877f0613a92fd68c29fc75e6a2fb6c2	aGVsbG8gaCByIHU=	0.00024294853210449
3	1	a71698d590eb6791392f770a45b51073	d4d1a60f8d365a55c8a3abf4065c09ec6409def0	aGVsbG8gaG93IHIgdQ==	0.39537596702576
3	3	f582339ce75b24996e5eadd71b316851	2fa9aaa270c169743dd17c3bba6cbfd0f605f06a	aGVsbG9ob3cgciB1Pw0K	0.00052213668823242
1	1	15b061bfdf98b81cee651c2b1d98e3b1	47ca001c1bf9de35181bfc606985aa6c131d17e3	SGVsbG8gSG93IHIgdSA/DQoNCkdvb2QgQWZ0ZXJub29u	0.00057005882263184
1	1	8b1a9953c4611296a827abf8c47804	f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf	SGVsbG8=	0.00018191337585

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

		d7	0		449
8	1	683aef499f82c9ea93624e9f4117a254	777b73064a6b6a1c981276ad2a35c5b68b75f817	aGVsbG8NCmdvb2QgbW9ybmluZw==	0.06371808052063
8	2	192ceeb80e05b8f14514801ec1fbc3fd	dd81b6bb040d72b522af0fb0aae18b2637ac4c7b	aHNkYTtzZGFdDQpzZGENCg0Kc2Rhc2RhDQpzZmRhDQpzZmdhDQoNCnNkDQoNCg0KDQoNCg0KDQoNCg0Kc2FnYQ0KYXNkDQphc2RnDQo=	0.000463962 55493164
9	2	f057f5ccb87a310534b9dda3a69a72c4	650f97e596e63e92d9447619d38e8a83e0bec8b9	aGlp	0.0014510154724121

References

[1] S.Bakhtiari, R. Safavi-Naini and J. Pieprzyk, 1995."Cryptographic hash functions: A Survey", Technical Report 95-09, Department of Computer Science, University of Wollongong.

[2] A.J. Menezes, P.C. Van Oorschot, S.A.Vanstone Handbook of Applied Cryptography, CRCpress, 1996.

[3] RSA Laboratories frequently asked questions about today's cryptography, version 4.1.2000. Available: http://www.rsasecurity.com.

[4] P. Rogaway and T. Shrimpton, 2004."Cryptographic hash-function basics: Definitions, implications and separations for preimage resistance, second-preimage resistance, and collision resistance", FSE 2004.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

[5] D.R. Stinson, 1994. "Universal hashing and authentication codes." Designs, Codes and Cryptography, 4, pp. 369–380.

[6] D.R. Stinson, 2006." Some observations on the theory of cryptographic hash functions" Designs, Codes and Cryptography, 38(2), pp. 259–277.

[7] Ilya Mironov, 2005. "Hash functions: Theory, attacks, and applications", J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.

[8] Nigel Smart, Cryptography: An Introduction. McGraw-Hill,Third edition,2003.Available: http://www.cs.bris.ac.uk/~nigel/Crypto_Book/

[9] I. Damgård, 1987. "Collision free hash functions and public key signature schemes", in: Proc. of Eurocrypt-87, in LNCS, vol. 304, pp. 203-216.

[10] I.B.Damgård, 1989 "A design principle for hash functions". In Gilles Brassard, editor, Advances in Cryptology: CRYPTO 89, volume 435 of Lecture Notes in Computer Science, pp. 416-427.

[11] B.Preenel, 1994."Cryptographic hash functions", Transactions on Telecommunications, VOL5, pp. 431-448.

[12] Bart Preneel, 1993."Analysis and Design of Cryptographic Hash Functions", Dissertation, Katholieke Universiteit Leuven.

[13] William Stallings. Cryptography and Network Security: Principles and Practice. Third edition, Prentice Hall. 2003.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

[14] W.Diffie and M.E Hellman, 1976. “New directions in cryptography”, IEEE Transaction on Information Theory. vIT-22 i6, pp. 644-654.

[15] NIST,2002, “Secure Hash Standars“,FIPS PUB 180-2.

[16] X. Wang, X. D. Feng, X. Lai and H.Yu, 2004. “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, rump session, CRYPTO 2004.

[17] R.L.Rivest, 1992.”The MD4 Message Digest Algorithm”,RFC 1320.

[18] R.L.Rivest, 1992.”The MD5 Message Digest Algorithm”,RFC 1321.

[19] RIPEMD, Research and Development in Advanced Communication Technologies in Europe, RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040), RACE, June 1992.

[20] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel, 1996.” RIPEMD-160– A Strengthened Version of RIPEMD”, Lecture Notes on Computer Science, Volume 1039, Fast Software Encryption 1996, pp. 71–82.

[21] X. Wang, H. Yu and Y.L. Yin, 2005. “Efficient Colision Search Attacks on SHA-0”, CRYPTO 2005.

[22] XiaoyunWang, Yiqun Lisa Yin, and Hongbo Yu, 2005.”Finding Collisions in the Full SHA-1, Lecture Notes in Computer Science, Volume 3621, Advances in Cryptology – CRYPTO 2005 Proceedings, pp. 17–36.

[23] Xiaoyun Wang, Andrew Yao, and Frances Yao, 2005.”New Collision Search for SHA-1, Presented at rump session of CRYPTO 2005.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

[24] K. Matusiewicz and J. Pieprzyk, 2006. “Finding good differential patterns for attacks on SHA- 1”, Lecture Notes in Computer Science, Volume 3969, pp. 164-177.

[25] NIST, “Secure Hash Standar“, 1995. FIPS PUB 180-1.

[26] Florent Chabaud, Antoine Joux, 1998. “Differential collisions in SHA-0,” Advances in Cryptology-CRYPTO’98.

[27] Eli Biham and Rafi Chen, 2004.”Near-Collisions of SHA-0”, Lecture Notes in Computer Science, Volume 3152, Advances in Cryptology – Crypto 2004 Proceedings, pp. 290–305.

[28] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, William Jalby, 2005. “Collision in SHA-0 and Reduced SHA-1”, Advances in Cryptology-EUROCRYPT 2005.

[29] Vincent Rijmen and Elisabeth Oswald, 2005.” Update on SHA-1”. In Alfred Menezes, editor, Topics in Cryptology - CT-RSA 2005, The Cryptographers’ Track at the RSA Conference 2005, San Francisco, CA, USA, volume 3376 of LNCS, pp. 58–71.

[30] Christophe De Cannière, Florian Mendel, and Christian Rechberger, 2007. “ Collisions for 70- Step SHA-1, On the Full Cost of Collision Search” , In Selected Areas in Cryptography, pp. 56- 73.

[31] Christophe De Cannière and Christian Rechberger,2008. “Preimages for Reduced SHA-0 and SHA-1”, In CRYPTO 2008, pp. 179-202.

[32] R.L.Rivest, 1992. “The MD2 Message-Digest Algorithm”, RFC 1319.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

[33] Bert den Boer and Antoon Bosselaers, 1991. “An Attack on the Last Two Rounds of MD4”, Lecture Notes in Computer Science, Volume 576, Advances in Cryptology – Crypto ’1991 Proceedings, pp. 194–203.

[34] Hans Dobbertin, 1996. ”Cryptanalysis of MD4”, Lecture Notes in Computer Science, Volume 1039, FSE 1996, pp. 53–69, February 1996.

[35] Hans Dobbertin, 1997. ”The First Two Rounds of MD4 are Not One-Way”, Lecture Notes in Computer Science, Volume 1372, FSE 1998, pp. 284–292.

[36] Bert Den Boer and Antoon Bosselaers, 1994. „Collisions for the Compression Function of MD5”, Advances in Cryptology, Proceedings Eurocrypt ’93, Springer-Verlag LNCS 765, pp. 293–304.

[37] Hans Dobbertin, 1996. “Cryptanalysis of MD5”, Rump Session, EUROCRYPT 1996.

[38] Vlastimil Klima, 2006. “Tunnels in Hash Functions: MD5 Collisions Within a Minute.”,Cryptology ePrint Archive, Report 2006/105, 2006.Available: http://eprint.iacr.org/.

[39] Yusuke Naito, Yu Sasaki, Noboru Kunihiro, and Kazuo Ohta, 2005.” Improved Collision Attack on MD4”, Cryptology ePrint Archive, Report 2005/151, May 2005. http://eprint.iacr.org/2005/151.pdf

[40] Yuliang Zheng, Josef Pieprzyk, and Jennifer Seberry, 1993.” HAVAL – A One-Way Hashing Algorithm with Variable Length of Output”, Lecture Notes in Computer Science, Volume 718, Advances in Cryptology – Auscrypt ’92, pp. 83–104.

[41] R.J.Anderson,.E.Biham., 1996. “TIGER: A Fast New Hash Function”,FSE, LNCS, vol. 1039, pp. 89–97.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012

[42] Paulo S.L.M. Barreto and Vincent Rijmen ,2000.” The Whirlpool Hash Function “, First open NESSIE Workshop.

[43] Eli Biham and Orr Dunkelman, 2006. “A framework for iterative hash functions-HAIFA”, NIST Second Hash Functions Work Shop, Santa Barbara.

[44] D. Hong, S. Jaechul, S. Hong, S. Lee and D. Moon, 2005. “A new dedicated 256-bit hash function: FORK-256”. First NIST Workshop on Hash Functions.

[45] H. Gilbert and H. Hanschuh, SAC 2003,“Security Analysis of SHA-256 and sisters, Selected Areas in Cryptography”, Ottawa, Canada, Lecture Notes in Computer Science, vol. 3006, M. Matsui and R. Zuccheratopp (Eds), Springer,2004, pp. 175-193.

[46] R. Merkle, 1989.” One way hash functions and DES. In: Brassard, CRYPTO 1989. LNCS, vol. 435, pp. 428–446. Springer, Heidelberg.

[47] H. Tiwari and K. Asawa, 2010, “A Secure Hash Function MD-192 with Modified Message Expansion”, IJCSIS, Vol. 7, No. 2, pp. 108-111.

[48] C. S. Jutla and A. C. Patthak, 2005. “A simple and provable good code for SHA message expansion”. In IACR ePrint archive 2005/247.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V2I4M2-072012
VOLUME 2 ISSUE 4 July 2012