A Secured Approach to Protect SIP Signaling Message

Narendra M. Shekokar
Dept. of Computer Engineering
D.J. Sanghvi College of Engineering
Mumbai, India
nshekokar@yahoo.co.in

ABSTRACT: *In today's era VoIP system is globally accepted and popular communication system because of its reach features. VoIP system uses two signalling protocol: H323 and SIP (Session Initiation Protocol). Out of these SIP is popular amongst VoIP subscriber because of its light weight nature, but SIP is vulnerable to various confidentiality threats because of its text nature and poor authentication. In this paper we have attempted to provide confidentiality to SIP signalling message by designing secured symmetric encryption algorithms to address the vulnerability of DES algorithms. Proposed algorithm is working on Feistel cipher principle. Proposed algorithm is tested based on its security strength.*

Keywords: SIP, VOIP, Confidentiality Threats, Symmetric Cipher Technique, DES Vulnerability

Received: 31 May 2014, Revised 3 July 2014, Accepted 10 July 2014

1. Introduction

Voice over IP (VoIP) is gaining more popularity in today's communication because of its rich multimedia feature and it is more economical compared to traditional PSTN (Public Telephone Switching System). SIP [1] and H.323 [2] are two major protocols in VoIP system, which are responsible to session initializing, management and termination. SIP becomes one of the dominant signaling protocols because of its light weight nature but is more prone to attacks and security threats as it uses HTTP digest technique for authentication and all messages are exchanged in open text. Confidentiality and availability threats are amongst most important threats on VoIP system causing over billing, force teardown and denial of service attacks.

In this paper, we have attempted to address confidentiality threats by proposing secure symmetric encryption technique compare to DES[3].Proposed algorithm uses 128 bit key instead 64 and also divide a 96 bit message block into 3 sub-blocks and use 2 functions f1 and f2 in each round. Each function uses different key (K1 and K2 respectively). For the key scheduling SHA 256 is performed on the initial key and also in successive rounds. We will also perform cryptanalysis of our algorithm to test its strength.

The paper is organized as follow: The section II deals with the existing architecture and call flow setup of SIP. In the section III addresses VoIP vulnerability and possible attack on of the paper we present some of the vulnerabilities and attacks possible on the SIP which affects the VoIP communication especially confidentiality and availability of the data. The section IV deals with the proposed algorithms for securing SIP signalling. Section V we analysed and tested proposed algorithms for its security strength. Finally, paper concluded in section VI.

2. VOIP Session Initiation

In VoIP system call setup is taking in two phase: session initiation and actual communication. SIP protocol is use during session initiation, while RTP is use for real time communication. SIP based VoIP system use four major components.

• Proxy Server which acts as both server and client and are responsible for the intermediate request and response generation [1].

• Registrar Server [1] registers the location of a user agent who has logged onto the network [1].

• Redirect Server allow users to temporarily change geographic location and still be contactable through the same SIP address [1].

• Location Server which gives the actual location of the UAC [1].

SIP uses following messages during session initialization and session termination [4].

In SIP for initiating a session between two terminals an invite message has to be sent by the calling party to the called party via the SIP proxies. The message first goes to the inbound proxy. The inbound proxy checks the policies such as the calling party is authorized to call or not. The inbound proxy communicates on behalf of the calling party.

This proxy also plays a vital role in forwarding the messages and also ensures that the messages are sent to the proxies nearer to the called party. The forwarding decision is taken based on the domain which is defined in unique SIP URI. The SIP URI identifies the target party. The message is forwarded to the proxy who is in the same domain as the called party. After receiving message the outbound proxy will forward message to the called party [1] [4].

Due to the text based nature of SIP, it is vulnerable to various threats. SIP vulnerabilities are listed as below.

• All SIP messages is exchange in clear text format, result of this is attacker can easily intercept and reuse the credential of major signaling message.

• HTTP Digest authentication protects user credential by using a cryptographic hash function (MD5), which is vulnerable to message digest attack.

• HTTP Digest authentication scheme supports one-way authentication of SIP message.

During session initialization INVITE message which carry credential information is in clear text message, this message is intercepted by attacker and obtaining necessary credential information to launch confidential attack on VoIP system.
Confidentiality refers to the protection of data from being read by an unauthorized user. Confidentiality threats on VoIP are listed as below.

• Force teardown attack

• Message altering

• Call Pattern Tracking

• Number Harvesting

Force Teardown attack: This attack is a result of interception of credential message from early communication and used later by attacker to send malformed message to victim machine.

Messaging altering: Invite message is alter by attacker during session initialization to divert the session to unauthorized recipient.

Call Pattern Tracking: This is an unauthorized analysis of VoIP traffic from or to any specific nodes or network so that an attacker may find a potential target device, access information (IP/port), protocol, or vulnerability of network. It could also be useful for traffic analysis [8].

Number Harvesting: Number Harvesting is the authorized collection of IDs, which may be numbers, strings, URLs, email addresses, or other identifiers in any form which represent nodes, parties or entities on the network [9].

INVITE	Session setup
ACK	Acknowledgement of final response to INVITE
BYE	Session termination
CANCEL	Pending session cancellation
REGISTER	Registration of a user's URI
OPTIONS	Query of options and capabilities
PRACK	Provisional response acknowledgment
UPDATE	Update session information
REFER	Transfer user to a URI
SUBSCRIBE	Request notification of an event
NOTIFY	Transport of subscribed event notification
MESSAGE	Transport of an instant message body

Table 1. SIP Method

SIP call flow is given in following Figure 1

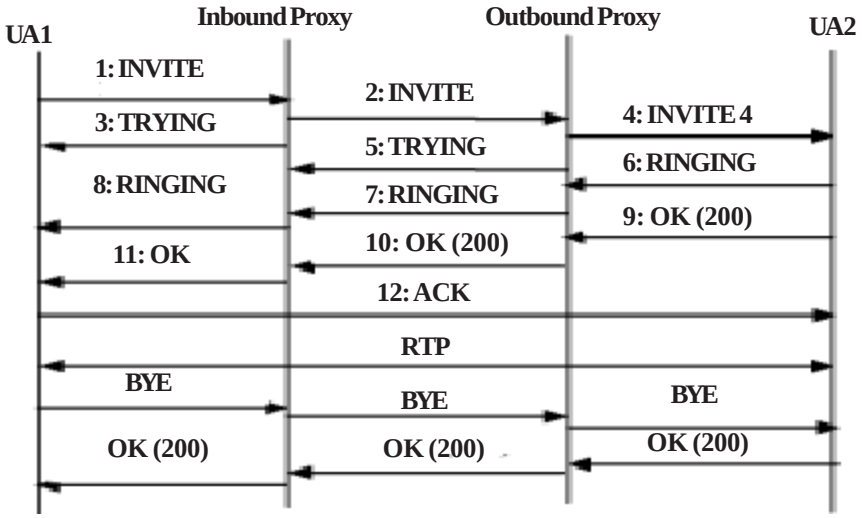

Figure 1. SIP Call Flow

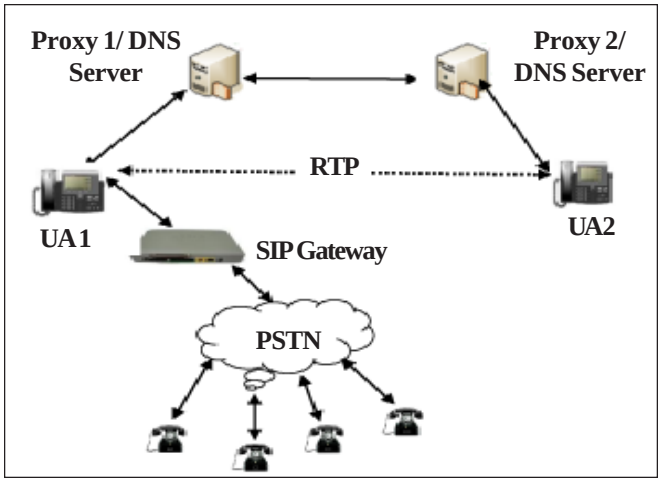

Figure 2. VoIP Proposed system

3. Proposed System

Proposed system architecture is given as below.

To provide the confidentiality to SIP signaling message, a secured tunnel need to establish between two communicate parties, an attempt has been made to propose a secured symmetric encryption algorithms.

3.1 Proposed Algorithms

Proposed algorithm is working on Feistal cipher technique, it overcomes the vulnerability of standard DES algorithm [6]. The standard DES algorithm is insecure because of following reasons.

- Small Key Length: 56 bits

- Susceptible Key Schedule: The user password directly becomes the key for the first round

The proposed algorithm removes several of DES's known vulnerabilities by doubling the key length, changing the internal operation and fortifying the key schedule using the SHA-512 algorithm, splitting the 512-bit hash key into two parts also ensures that consecutive round keys are not interdependent.

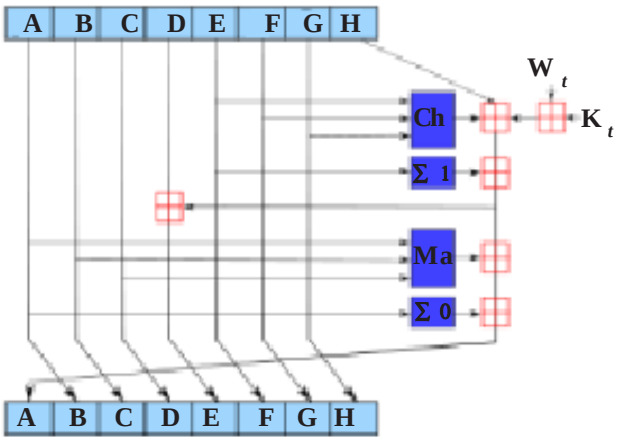

Figure 3. Hashing algorithm

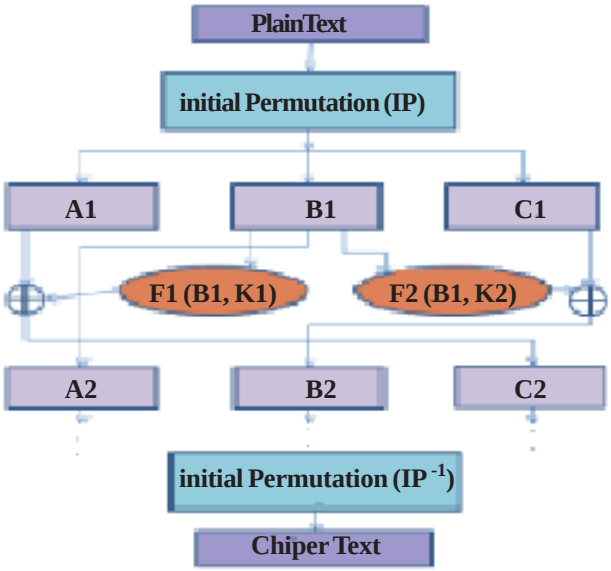

Figure 4. Single cycle of proposed algorithms

3.1.1 Proposed Algorithm

Pre-encryption in SVKT algorithm Initially the user enters a password which will be used as the input to key generator. The entered password is divided into 8 blocks and performs SHA-512 operations on it to generate a new 512 bit hash key.

SHA 512 is a very strong hash function and has not been broken so far. It is a one way hash and takes in a string of any length and returns a hash key of 512 bits. It uses 8 chaining variables A to H. These chaining variables are initialized in the beginning to 32 bit values. The hash key produced at the end of 64 rounds is unique for every message. Also, this algorithm exhibits the avalanche effect i.e. with a small change in the message there is a considerably large change in the final hash value. However, because of its complex internal operations, it has not yet been successfully attacked by cryptanalysts.

3.1.2 SVKT Key Modification

The 512 bit hash key is divided into 4 parts of 128-bit keys, these keys are use during 4 rounds. This approach of key generation eliminates DES weakness of interdependence of round keys. After every 4 rounds, the keys are modified using the SHA-512 algorithm. Decryption can be achieved by simply reversing the encryption steps.

In each round 128 bit key is divided into two part of size 64bit, which is pass through the DES S-boxes to generate 96 bit round keys. These keys ($K1$, $K2$) are uses in round 1 and round 2 respectively.

3.1.3 Internal Working of SVKT Rounds

Instead of the standard 56 bit key of DES proposed algorithm uses a 128 bit key. Proposed algorithm encrypts 96 bits of data at a time as against 64 bit in the earlier versions. To improve security of algorithms standard Feistel cipher technique has been modified.

Steps:

1) The 96 bit block will be divided into 3 blocks of 32 bits each (A, B, C).

2) We will use the 8 S3 S-boxes (S1 to S8). These S-boxes are resistant to linear and differential cryptanalysis.

3) In each round, the generated 128 bit key is divided into two parts (K1 and K2) and the appropriate function is performed.

4) The same function is used with two different 56 bit keys (reduced from 64 bit) is used in each round.

5) The operations are as follows:

Encryption:

$A(i) = B(i-1)$

$B(i) = C(i-1)\ XOR\ f\ (B(i-1), K(2, i))$

$C(i) = A(i-1)\ XOR\ f\ (B(i-1), K(1, i))$

Decryption:

$A(i-1) = C(i)\ XOR\ f\ (A(i), K(2, i))$

$B(i-1) = A(i)$

$C(i-1) = B(i)\ XOR\ f\ (A(i), K(1, i))$

$f1\ (B(i-1, K(1, i)) = P(S1(D1), \ldots.. S8(D8))$

$f2\ (B(i-1), K(2, i)) = P(S1(D9), \ldots. S8(D16))$

Proposed Symmetric encryption algorithm established secured tunnel between UA's and proxies, result of this all signaling messages exchange in secured way between them. Integrity of signaling message is protected using SHA-1 [10].

SIP message contain two part SIP Header and SIP Body. SIP Header contain following fields,

- Message type (INVITE, OK, BYE and CANCLE)
- Via

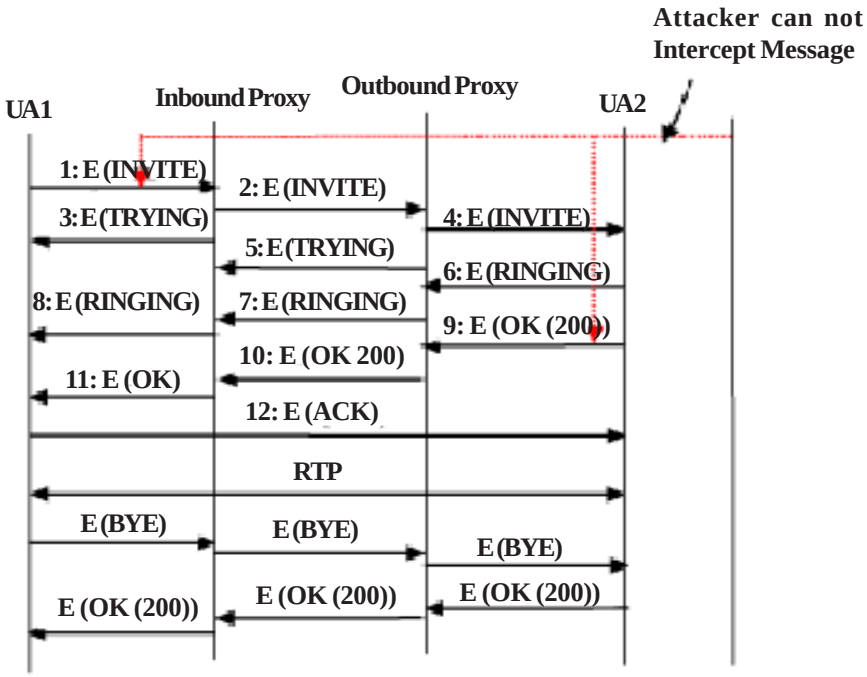

Figure 5. Secured SIP Call Flow

• Max-Forwards

• Route

• From

• TO

• Call-ID

• Cseq

• Contact

• Proxy-Authorization (Digest name, relam, nonce, URI, response),

• Response is calculated by applying message digest on relam, nonce, userid, password theses credential are used by proxy/ registrar server to authenticate UA.

• Content-type

• Content-Length.

SIP Body contains SDP (Session Description Parameter). Contents of SDP are listed as below.

• V (version of SDP)

• (Owner/creator and session identifier, session version address)

• S (Session subject)

• C (Connection information)

• M (Media description: type, port, possible formats caller is willing to receive and sends)

All SIP header fields except response is kept in clear text format, in our proposed technique response is calculated by applying SHA-1 algorithms. SIP Body is encrypted using symmetric encryption technique.

Format of the SIP message sends by UA1 to proxy server is given in Figure 6.

SIP Header	SIP Message Body

Figure 6. SIP Message Format

Contents of SIP Header are given as below.

SIP Header = { SIP Header Fields || Mdc}

Details field of SIP Header are given as below.

SIP Header - > ("*Message Type*", To, From, CSeq, *Call _ ID*, Contact, *max _ forwards*, date, contect, content type, content- Length, || Response)

Response field of SIP Header is called as *Mdc* which is generated by applying hash function (SHA-1) on nonce, relam, userid and password. Format of *Mdc* is given as below,

Mdc = Hash (nonce, relam, userid, password)

Format of SIP Message Body is given as below.

$$SIP\_MSG\_Body\text{->}\ (IDA \,||\, H\,(SIP\_MSG) \,||\, E\,(SIP\_MSG)_{K1})$$

H = Hash Algorithms (SHA-1), *K*1 = symmetric key agreed by UAS and Proxy Server.

SIP_MSG_Body contains message digest *H* (*SIP _ MSG*) and encrypted message (*SIP _ MSG*) *K*1. *SIP* message digest is generated by applying SHA-1 hashing algorithm on entire SIP message, while encrypted message is generated by applying proposed encryption technique on entire *SIP* message. As UA2(receiver) receive the *SIP* message, first UA2 will decrypt the message and then new message digest is calculated by applying SHA-1 on decrypted message, message is accepted by UA2 only if old message digest H(SIP_MSG) is match with new message digest.

4. Cryptographic Analysis

Proposed encryption technique is cryptographically analyze using CRYPTOOL based on factor Entropy, Histogram and *N* gram.

4.1 Entropy

Entropy is calculated based on randomness, mathematical disfiguration and obfuscation. Entropy is the measure of uncertainty associated with a random variable.

4.2 Histogram

A histogram is a graphical representation showing a visual impression of the distribution of data. It is an estimate of the probability distribution of a continuous variable.

4.3 N gram

An *n-gram* model is a type of probabilistic language model for predicting the next item in such a sequence. The two core advantages of n-gram models are relative simplicity and the ability to scale up – by simply increasing n a model can be used to store more context with a well-understood space–time tradeoff, enabling small experiments to scale up very efficiently.

• Analysis of 3DES

INVITE message of VoIP:
14:33:14.710 Wed 28 Mar 2012, 92.168.29.12:5060/udp (373 bytes): sent INVITE sip:alice@192.168.29.12:5070 SIP/2.0 Via:SIP/2.0/UDP

192.168.30.118:5080;rport;branch = z9hG4bK90155 Route: <sip:192.168.29.12;lr> Max-Forwards: 70 To: Alice <sip:alice@192.168.29.12>; From: Bob

<sip:bob@192.168.29.12>;tag=z9hG4bK60492682 Call-ID: 308705092944@192.168.30.118 CSeq: 2 INVITE User-Agent: mjsip stack 1.6 Content-Length: 0

Cipher text generated using 3 DES (Invite Message)

253ad5b03bf535014baedfc4d1ff01fa21ab521f1e427a7c9729 31d644c46883f239a19e07c193fe895e21421d5cb764cc13cf3
4a5691a0318da293d234b8fa5c2ed5c76ad8fac49c27179c80 61b12c2fc5faea8abf1b969b8bda0586a2738eb231ca25638c1f
af3ceafd8d6380e389c54c259aaa7410a231ea4c3c3014f945f 3a107da8b2f5e59e312225d8c4b1fd108e1142dac5f647dd4fa
573e4ca9e0e244117ee32988524d9ae21096d4190d8be01311 253ad5b03bf535014baedfc4d1ff01fa21ab521f1e427a7c97293
1d644c46883f239a19e07c193fe895e21421d5cb764cc13cf34a 5691a0318da293d234b8fa5c2ed5c76ad8fac49c27179c8061b
12c2fc5faea8abf1b969b8bda0586a2738eb231ca25638c1faf3c eafd8d6380e389c54c259aaa7410a231ea4c3c3014f945f3a107
da8b2f5e59e312225d8c4b1fd108e1142dac5f647dd4fa573e4c a9e0e244117ee32988524d9ae21096d4190d8be01311e8565fb
15c5793126721ed94d7fea915d02ab88a31b562beda8ba54bc 0486d0ca4609f6e166bdcfaa41a378bd833a5e27cccb6cf7dc63
454f44a5a172fcedfa43958e5351e07e32551594952b0e6f7cc 03f7354024a4ace1b3c006a50f2d1dadc4353dc9a708e257e168
24765bd303d0bc960eb1f598ba0d1c0bece3b46f46ed80a1f4a5 50b18acd5c48e1d82328ec99ee5fdd4857dbddb489decbcdba
635dc5dd82d3a0c2410eb58dc2bd27b56987d20972a33043c26 1357ed22cb1fc680bf5b2b724cd41e5753d1df5a6891f9085cc
7963a6b6b41e7e0a97ce0ac5d5dbb208c3f9c83b5b6b63d8018 d2090cf7a444fa66f

Analysis of Proposed Encryption Algorithm

Cipher Text generated using proposed encryption algorithms

281fd3de9f32816a10a2e6500cc4288cb2dad6720dbeb26aa0c2 92ba4c1a51377b6380c3a86b676a65393e26263d1684a2363bd
59f272422a6389070649a889434038bcaea6d009c022a41f50 0dd6fb83050e1e820fc5ef971025c03ec43b5eeab0523f38bc42
d1bc593f9a82387d8a10e950faea77c879014e7afade57e0599 e301f6c466c020f56869adce5d20aa8f0ba50340a4708bfc876d
753bd0634e90f3069f93f2fe825c6d1789151816ba8dd2ed682f 141d712fd920e6e71ed039acbb15611da3e6129622ffd20a481
f143094077f3919bbd6a7eefdf4bcdbcb94deced1b85f1e90fd96 6ee74543b36f09b36694c1e9efecf059895f71203cfb6c7667d3
036469e3ecb62e9b34d20d32f7b587700d55b144121957086a6 92f84ffa8dba4e0813e6237f529f91fbd0f0b105e8b0f8148e665
7eac069263899d4dc576c40bf8e88e17a2418ff24e861ed9b80 394f99b96c85c3854e05457de4ac6aa5255f2a249c2886c78ec5
cd8b072f855cc11ac5777310e4637af8f248cdb557cd8a8a937 e9bc8cd21ce97a726a4704abccb1fb06d4cc31b025faf974f62e7
afa92744593c8aebe232490a43e760f

Analysis of two techniques was carried out based on features Entropy, Histogram, Digram and Trigram. The result shown in the table proves that proposed encryption algorithms give close value of entropy and frequency range to 3DES. The high value of Entropy indicates that there is a high randomness in cipher text and also it is tougher to crack.

The proposed Encryption technique gives a better range of Digram as compared to the 3DES, hence indicating a better distribution of dual sequences of character.

Entropy analysis of cipher text generated using 3 DES

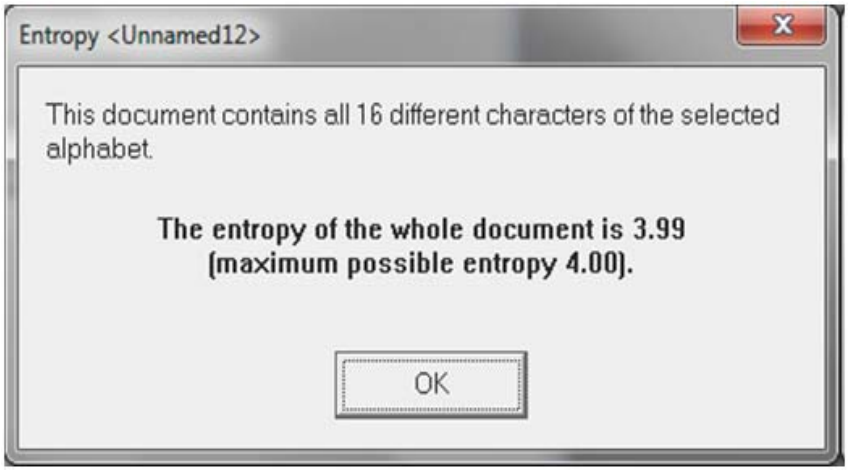

Figure 7. Entropy of cipher text (3DES)

5. Conclusion and Future Scope

VoIP system confidentiality threats has been analyze and attempt has been made to deter it by providing secrecy to all signaling messages by using symmetric encryption algorithms. Performance of proposed algorithms is compared with well known symmetric encryption technique. Integrity of signaling message is maintained by using non breakable hashing technique. Security analysis of proposed encryption is carried out using Cryptool based on factor Entropy, Histogram Digram and Trigram. Result of crypto analysis shows that proposed algorithm is provides close result to 3DES.

To improve proposed algorithm to obtain better result as compare to 3DES is our future work.

Histogram of cipher text generated using 3DES

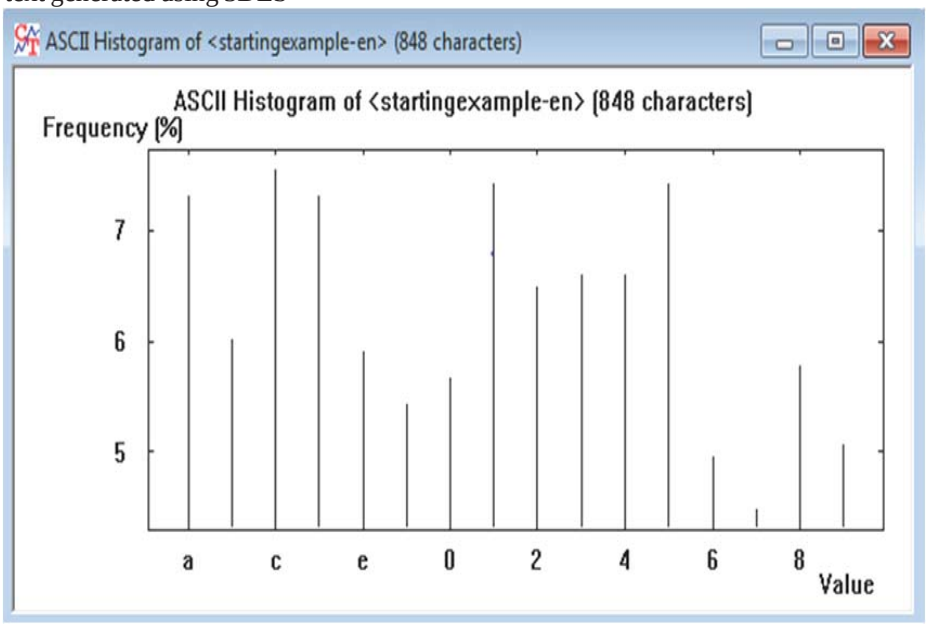

Figure 8. Histogram of cipher text (3DES)

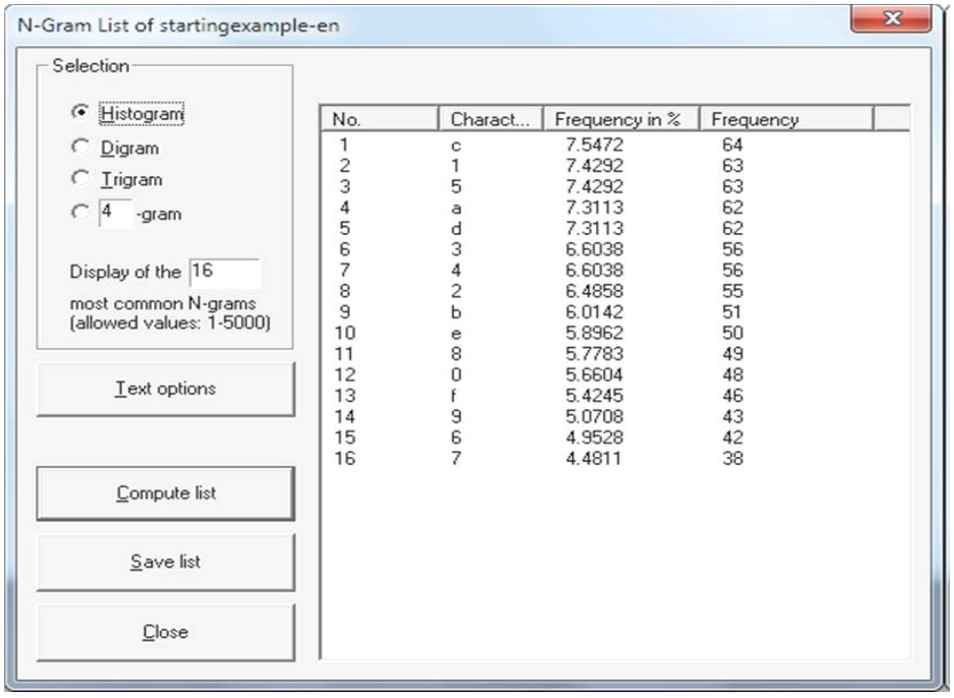

Figure 9. N-Gram analysis of cipher text (3DES)

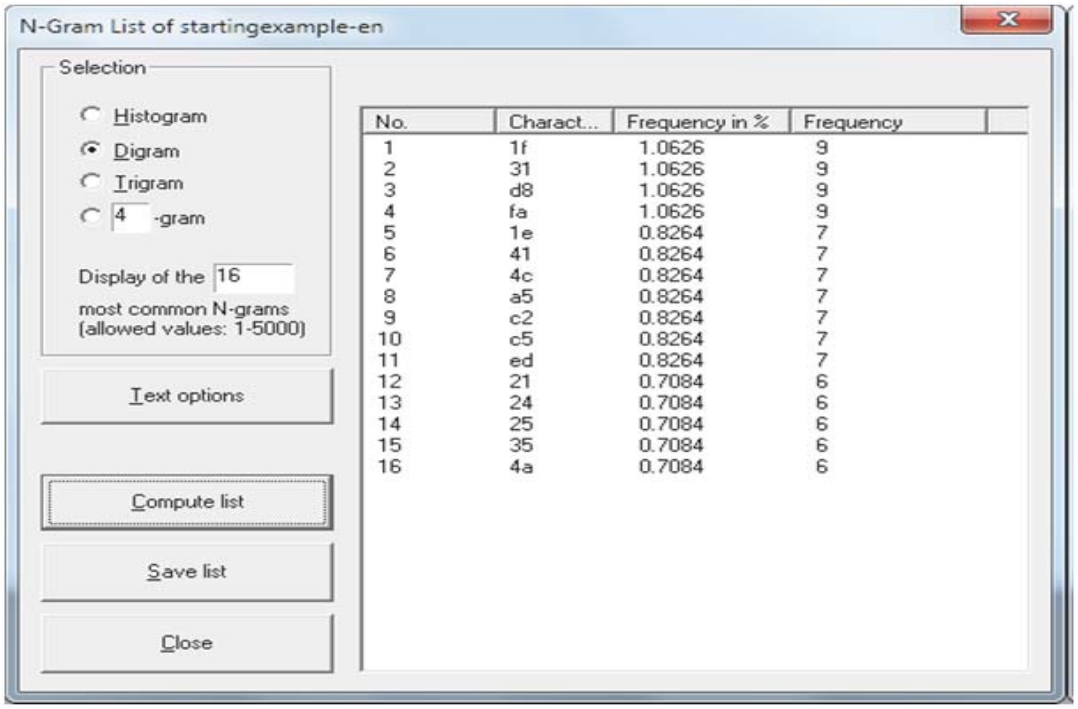

Figure 10. Diagram analysis of cipher text (3DES)

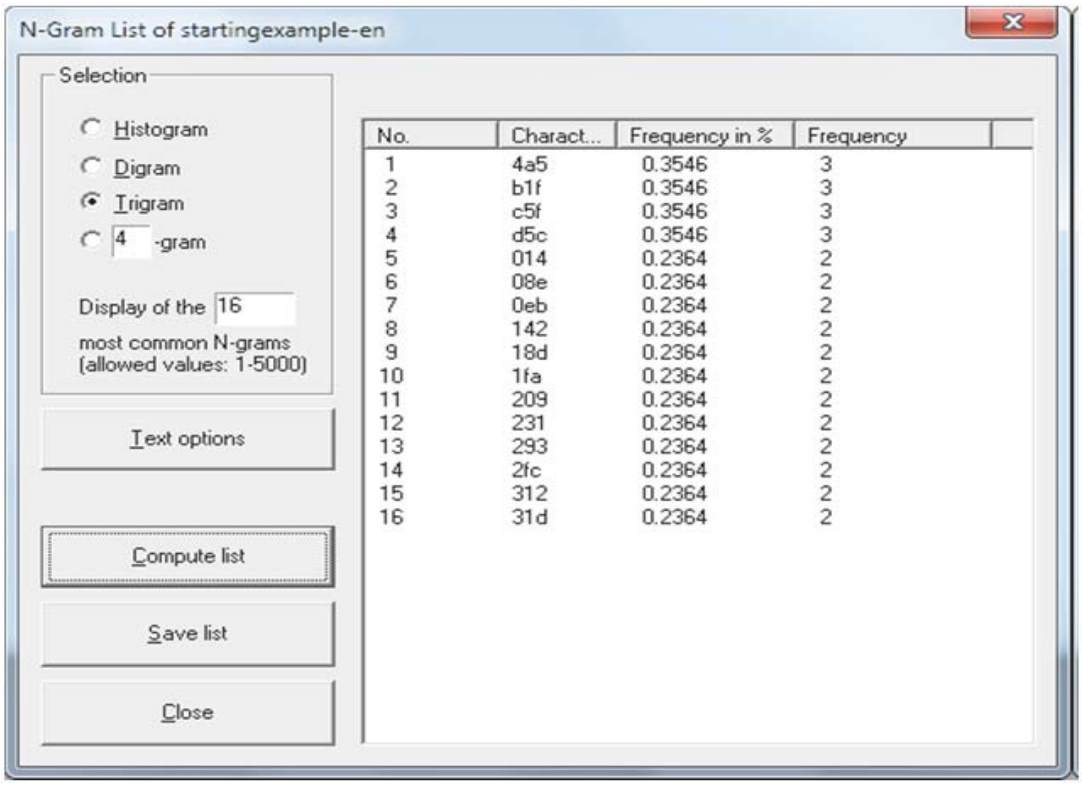

Figure 11. Trigram analysis of cipher text (3DES)

Entropy of cipher text generated using Proposed Encryption Algorithm

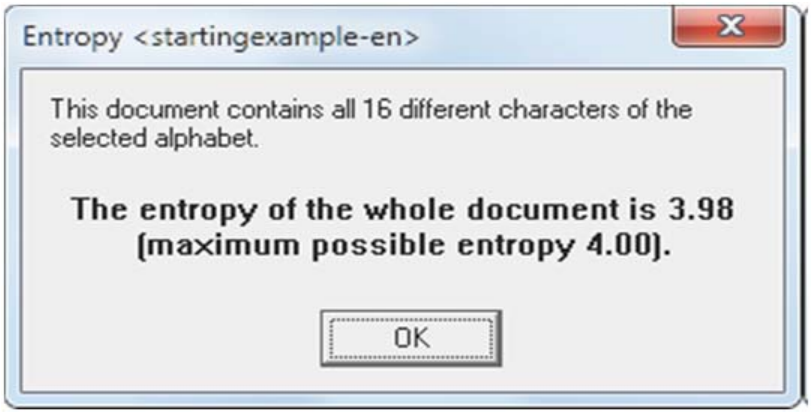

Figure 12. Entropy of cipher text (Proposed Algo.) Histogram

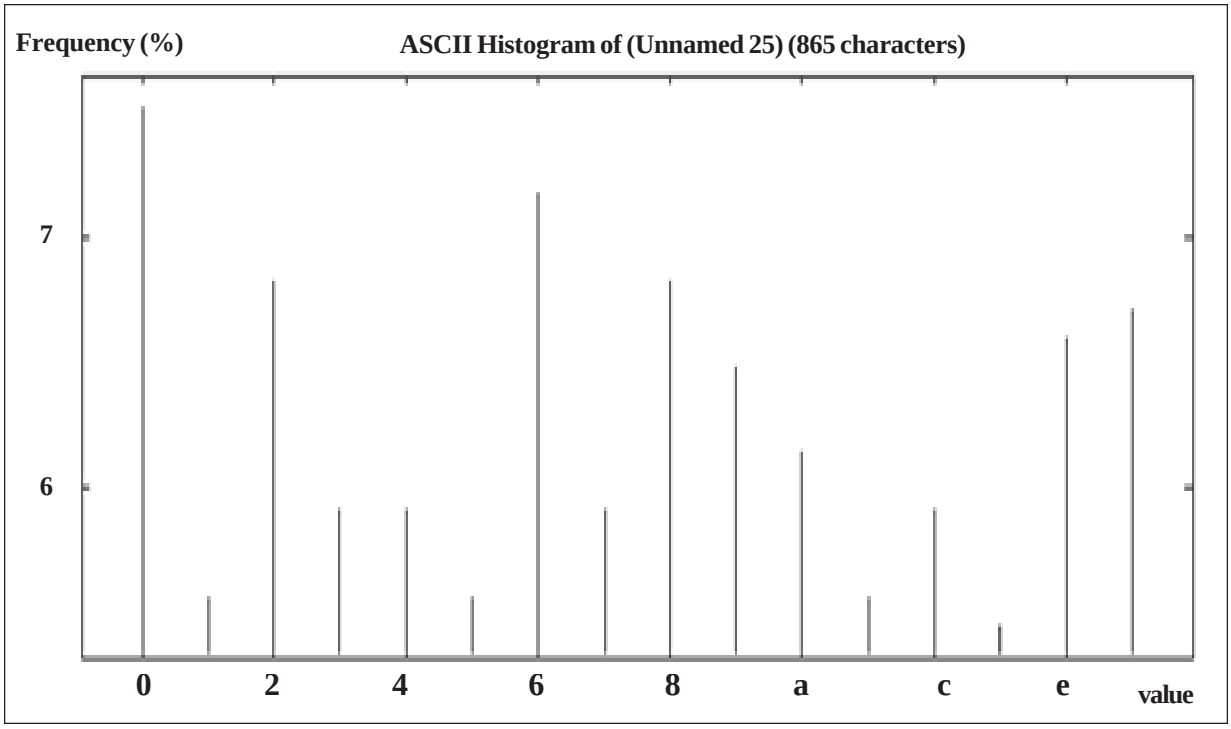

Figure 13. Histogram of cipher text (Proposed Algo.)

Sr. No	Text Type	Entropy	Histogram frequency range	Diagram range	Trigram range
1	Invite Message (Plain Text)	3.48	217-8	35-15	30-9
2	Cipher Text generated using 3DES	3.99	64-35	9-6	3-2
3	Cipher Text generated using Proposed algo.	3.98	65-47	8-6	3-2

Table 2. summary of cryptool analysis

Histogram analysis of cipher text generated using Proposed Encryption Algorithm

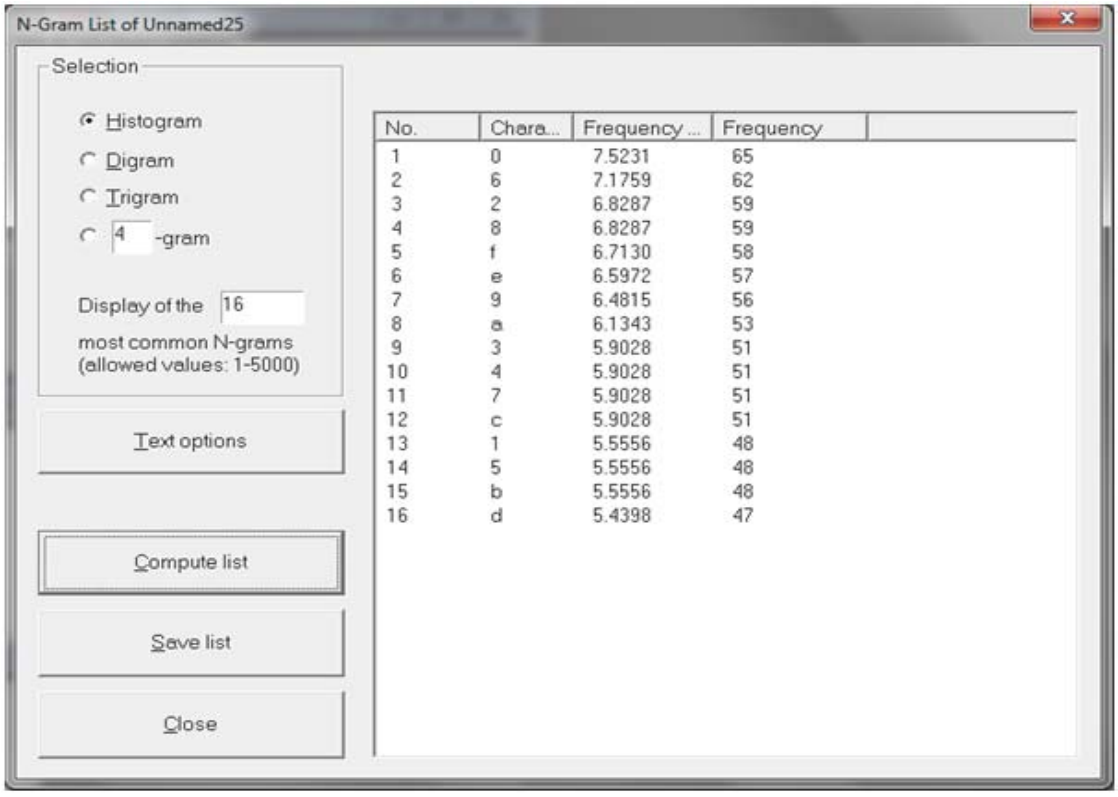

Figure 14. Histogram analysis of cipher text (Proposed Algo.)

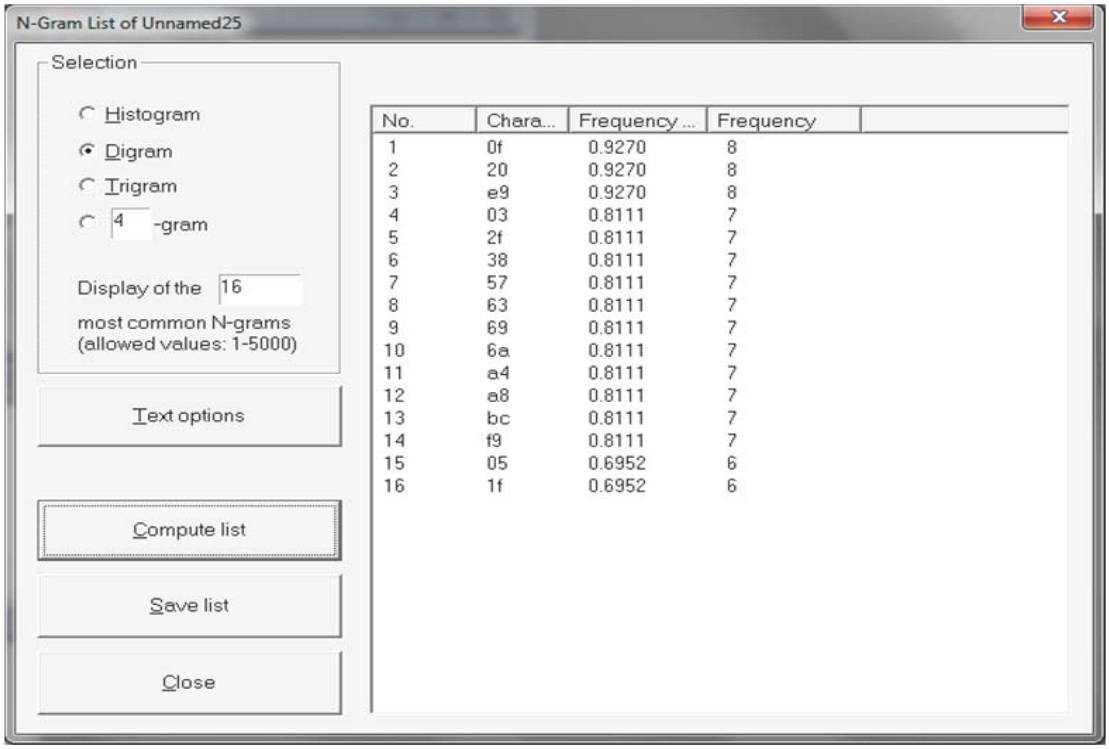

Figure 15. Diagram analysis of cipher text (Proposed Algo.)

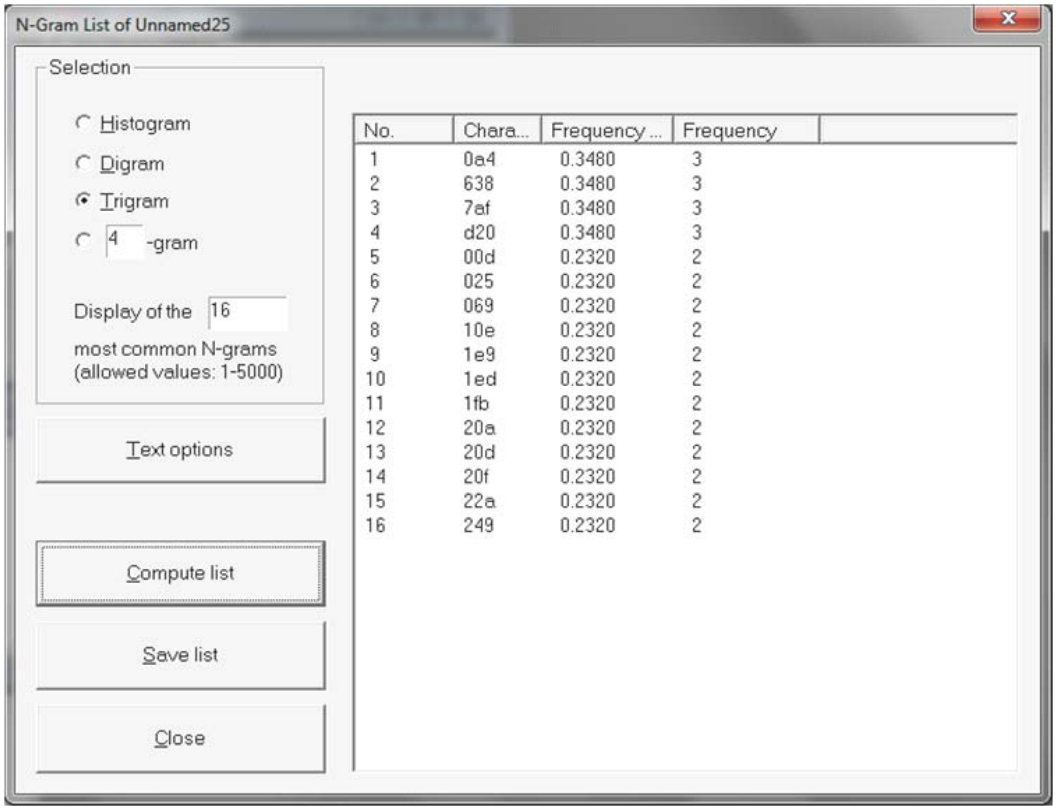

Figure 16. Trigram analysis of cipher text (Proposed Algo.)

References

[1] Rosenberg, J., Schulzrinne, H., Camarillo., G. Johnston., A. Peterson, J. Sparks., R. Handley., M. Schooler., E. (2002).SIP:SessionInitiation Protocol. RFC 3261 (Proposed Standard), June.Updated by RFCs 3265, 3853, 4320, 4916, 5393.

[2]Rec, I. H. 323, Packet based Multimedia Communications Systems [Online].Available: http://www.itu.int/rec/T-REC- H.323.

[3] Nimmi Gupta . (2012).Implementation of Optimized DES Encryption Algorithm upto 4 Round on Spartan 3, *IJCTEE*, 2 (1) 82-86.

[4] Schmidt, Holger., Dang, Chi-Tai ., Hauck, Franz J. (2007).Proxy-based Security for the Session Initiation Protocol (SIP) IEEE.

[5] Sinnereich., H. Johnston., A. (2006). Internet Communications Using SIP: Delivering VoIP and Multimedia Services withSession Initiation Protocol, Indiana: Wiley Publishing Inc., p. 103.

[6]Vidya, S., Chitra., K. (2013). Format Preserving Encryption using Feistel Cipher, International Conference on Research Trends in Computer Technology, ICRTCT-2013, *In*: *Proceeding of International Journal of Computer Application (IJCA)*, p.5-8,year

[7] Kulkarni., V. R. Dr.Apte., S. S. Alternate Approach for Implementation of SHA-2 Algorithm using Feed Forward Neural Network, *International Journal of Computer Application* (IJCA), 28, (5), p.30-34

[8] Shekokar, Narendra., Devane, Satish. (2010). A Novel Approach to Avoide Billing Threats WSAT,Penang Malaysia, 24-26 February.

[9] VOIPSA : VoIP Security and Privacy Threat Texonomy [online] http://www.voipsa.org/VOIPSA_Taxonomy_0.1.pdf ,24 October. 2005

[10] Khate., A. (2004). Cryptography and Network Security, Tata McGraw Hill, year 2004.