International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.1, No.1, July 2012, pp. 6~19
ISSN: 2252-8776

Novel TEA Algorithm for IP Telephony System

Samah Osama M. Kamel, M. Saad El Sherif , Adly S. Tag El Dein, Sahr Abd El Rahman
Computers & systems dept., Electronics Research Institute
Electrical Engineering Department- communication and computer branch
Benha University- Faculty of Engineering

Article Info

Article history:

Received May 19th, 2012
Revised June 01th, 2012
Accepted June 10th, 2012

Keyword:

Key derivation
SRTP session
SRTP session authentication
TEA
Encryption decryption
PRF: pseudo random function.

ABSTRACT

IP telephony that transmit voice calls over an IP network such as the Internet, IP telephony are growing very fast replace the traditional circuit switched infrastructure for telephony services. So we must protect all data that are transmitted from all attacks. To implement this process, the voice is encrypted, authenticated and decrypted to get the original data. The paper examines and evaluates the six encryption algorithm to minimize delay time to achieve minimum encryption time. A Novel TEA encryption Algorithm is examined for the minimum processing time to be suitable for IP Telephony which takes minimum time

Corresponding Author:

Samah Osamah M. Kamel,
Computers & Systems dept., Electronics Research Institute,
El Behoth Str.- National Research Center - Doki – Giza – Egypt.
Email: samah_n2003@yahoo.com

1. INTRODUCTION

IP Telephony is transport of telephone calls over the Internet and It has been rapidly replaced public switched telephone networks (PSTN). There are three protocols of IP Telephony which are signaling protocol (H.323 and SIP), media transport (RTP and RTCP) which transmits voice samples and Supporting Services (DNS, ENUM, TRIP, RSVP and STUN) which improves performance and ease of use. The Real Time Protocol (RTP) is used to transport voice media and it carried encoded voice message between two callers. It must protect RTP packet from many attacks in the network. This paper will discuss the implementation of SRTP in minimum time by using a novel TEA encryption Algorithm which takes minimum processing time.

In the first we used key derivation to implement SRTP that the key derivation function is used to derive the different keys used in a crypto context (SRTP encryption keys and salts, SRTP authentication keys) from one single master key in a cryptographically secure way. Thus, the key management protocol needs to exchange only one master key, all the necessary session keys are generated by applying the key derivation function. The master key and master salt provide by an external key management protocol as input to PRF to derive a set of session key. The set of session keys are session encryption and salt keys which are used to generate the keystreams that used for encryption/decryption SRTP packet and session authentication key is used to calculate and prove the MAC of the SRTP and SRTCP packets. We will discuss it in section 3.1.

The scenario of SRTP implementation consists of three steps. The first step is in the SRTP sender that the SRTP encryption and salt keys are used for the encryption and decryption SRTP packet which encrypt the RTP payload to produce the encryption portion of the packet by using a novel TEA encryption algorithm that it will be discussed in details in section 2.6.

The second step is authentication process to authenticate encrypted SRTP packet. The message authentication is used to calculate and prove HMAC of the SRTP packets. The sender side computes authentication tag for authenticated portion of the packet. In the SRTP receiver side will generate HMAC and compare between authentication tags in the SRTP sender side if two tags are equal, then message ||

authentication tag pair is valid otherwise; it is invalid and error audit message "AUTHENTICATION FAILURE" must be returned which will discuss in details in section 3.3.

The final step is in the SRTP receiver side which will decrypt the encryption portion of the packet by using novel TEA encryption algorithm in section 2.6. In Fig. 1 shows us SRTP implementation in short time.

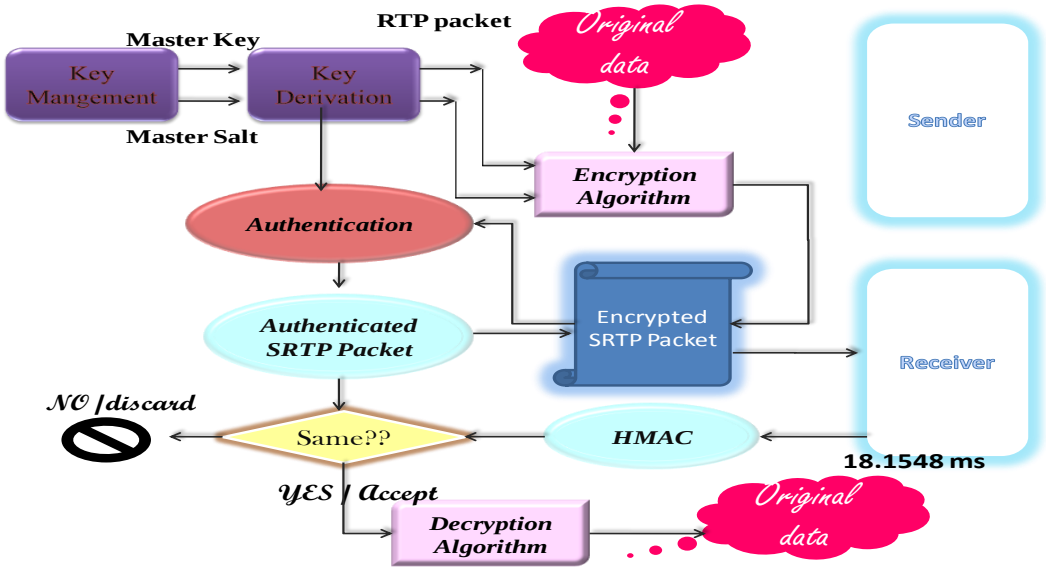

Figure 1. SRTP implementation in short time in ms.

To select the algorithm which takes minimum time, we must evaluate and compare among six encryption algorithms to minimize the processing time and we select the algorithm which will take less time. There are many examples of encryption algorithms such as AES, Blowfish, IDEA, RC5, CAST-128 and TEA. The strength of symmetric key encryption depends on the size of keys, number of rounds and the round function. For example, for longer key is the hardest to break or attack. The comparison will examine the processing time of the six encryption algorithms to minimize the processing time. Our paper will examine a Novel TEA Algorithm that it will take less time.

There are two encryption algorithm categories: symmetric and asymmetric key algorithms. Symmetric key algorithm bases on a shared secret and Asymmetric key algorithm bases on pairs of two types of keys private and public. Symmetric encryption algorithms are divided into stream ciphers and block ciphers, stream ciphers encrypt a single bit of plaintext at a time but block ciphers take a number of bits and encrypt them as a single unit.

AES is a symmetric key encryption technique which will replace the commonly used Data Encryption Standard (DES). AES is a block cipher which uses three key sizes: a 128, 192, or 256 bit encryption key. In each encryption key size causes the algorithm to behave a little differently, so the increasing key sizes not only offer a larger number of bits with which you can march the data, but also increase the complexity of the cipher algorithm. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. AES is based on a design principle known as a substitution permutation network and AES doesn't use a Feistel network. AES has a fixed block size of 128 bits and key sizes in any multiple of 32 bits with a minimum of 128 bits. The blocksize has a maximum of 256 bits but the keysize has no theoretical maximum and AES operates on a 4×4 column major order matrix of bytes termed the state. Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds which convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps including one which depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key [12].

Blowfish is a symmetric block cipher just like DES or IDEA which designed by Bruce Schneier 1993. It takes a variable length key, from 32 to 448 bits. The algorithm consists of two parts one of them is a key expansion part and a data encryption part and the other Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish encrypts 64 bit blocks into 64 bit blocks of cipher

text. Blowfish is based on Feistel rounds, and consist of the f function used amount of the facilitation of the principles used in DES to provide the same security with greater speed and efficiency in software [8].

IDEA was developed by Dr. X. Lai and Prof. J. Massey in Switzerland in the early 1990s to replace the DES standard. IDEA uses the same key for encryption and decryption. IDEA encrypts a 64 bit block of plaintext to 64 bit block of ciphertext and it uses a 128 bit key. The algorithm consists of eight identical rounds and a half round final transformation. It is a fast algorithm and has been done in hardware chipsets making it even faster [8], [11], [16], [34].

RC5 was developed by Ron Rivest which is block cipher and it is fast that is a simple algorithm and its word oriented the basic operation work on full word of data at a time. It encrypted block of plain text of length 64 bits into blocks of ciphertext of the same length and key length range from 0 to 2040 bits [8], [6].

Cast-128 was developed by Carlisle Adams and Stafford Tavares and key size varies from 40 bits to 128 bit increments. CAST-128 has structure of classical feistel network which consisted of 16 rounds and 64 bit blocks of plaintext to produce 64 bit blocks of ciphertext. CAST-128 has two subkeys in each round (32bit of km (i) and 5 bit kr (i)) and the function F depends on the round [3], [4], [5], [8].

The Tiny Encryption Algorithm (TEA) was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory. It is a symmetric private key encryption algorithm and TEA one of the fastest and most efficient cryptographic algorithms in existence and TEA operates on 64 bit blocks and uses a 128 bit key. It has a Feistel structure with a suggested 64 rounds, typically implemented in pairs termed cycles and TEA has an extremely simple key schedule, mixing all of the key material in exactly the same way for each cycle. The Feistel network uses a group of bit shifting XOR, and adds operations to create the diffusion and confusion of data [19], [20], [25].

2. THE COMPARISON BETWEEN SYMMETRIC CRYTPGRAPHIC ALGORITHMS

2.1. ADVANCED ENCRYPTION STANDARD (AES)

The input to the AES encryption and decryption algorithms is a single 128 bit block, depicted in FIPS PUB 197, as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output. The key is expanded into 44/52/60 lots of 32-bit words, with 4 used in each round. The data computation consists of an add round key step, then 9/11/13 rounds with all 4 steps, and a final 10th/12th/14th step of byte subs + mix cols + add round key. This can be viewed as alternating xor key and enter data bytes operations. All of the steps are easily reversed and can be efficiently implemented using xor's and table lookups [12].

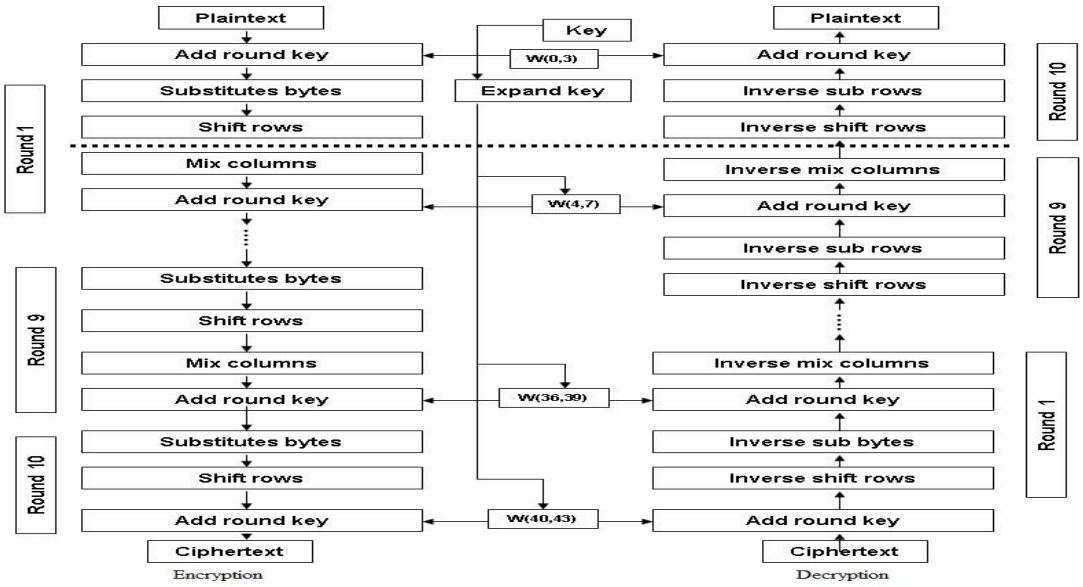

Figure 2. AES Encryption and Decryption.

The Simulation by matlab:
m= secure IP Telephony
E= ÈBa êºÓ1ü
D= secure IP Telephony
Elapsed time is 92.06 ms

2.2. BLOWFISH ALGORITHM

For encryption algorithm: the plain text is divided into two 32 bit halves LE0 and LR0. We have use variable LE(i), RE(i) to refer to the left and right half of data after round i has computed. Each round contains the complex use of addition modulo 2^32 and XOR, plus substitution using S boxes, the cipher text is includes in the two variable LE17 and RE17.

RE(i) = LE(i-1) xor P(i)

LE(i) = F[RE(i)] xor RE(i-1)

Where: F[a, b, c, d] =((S1,a + S2,b) xor S3,c) + S4,d

For decryption algorithm: the 64 bits of cipher text are initially move to the two one word variable LD(0) and RD(0). We use the variable LD(i) and RD(i) which refer to the left and the right half of data after round i. With most block ciphers, Blowfish decryption entails using the subkeys in reverse order. It isn't like most block ciphers; Blowfish decryption takes the reverse direction of the encryption.

RD(i) = LD(i- 1) xor P(19-i)

LD(i)= F[RD(i)] xor RD(i-1)

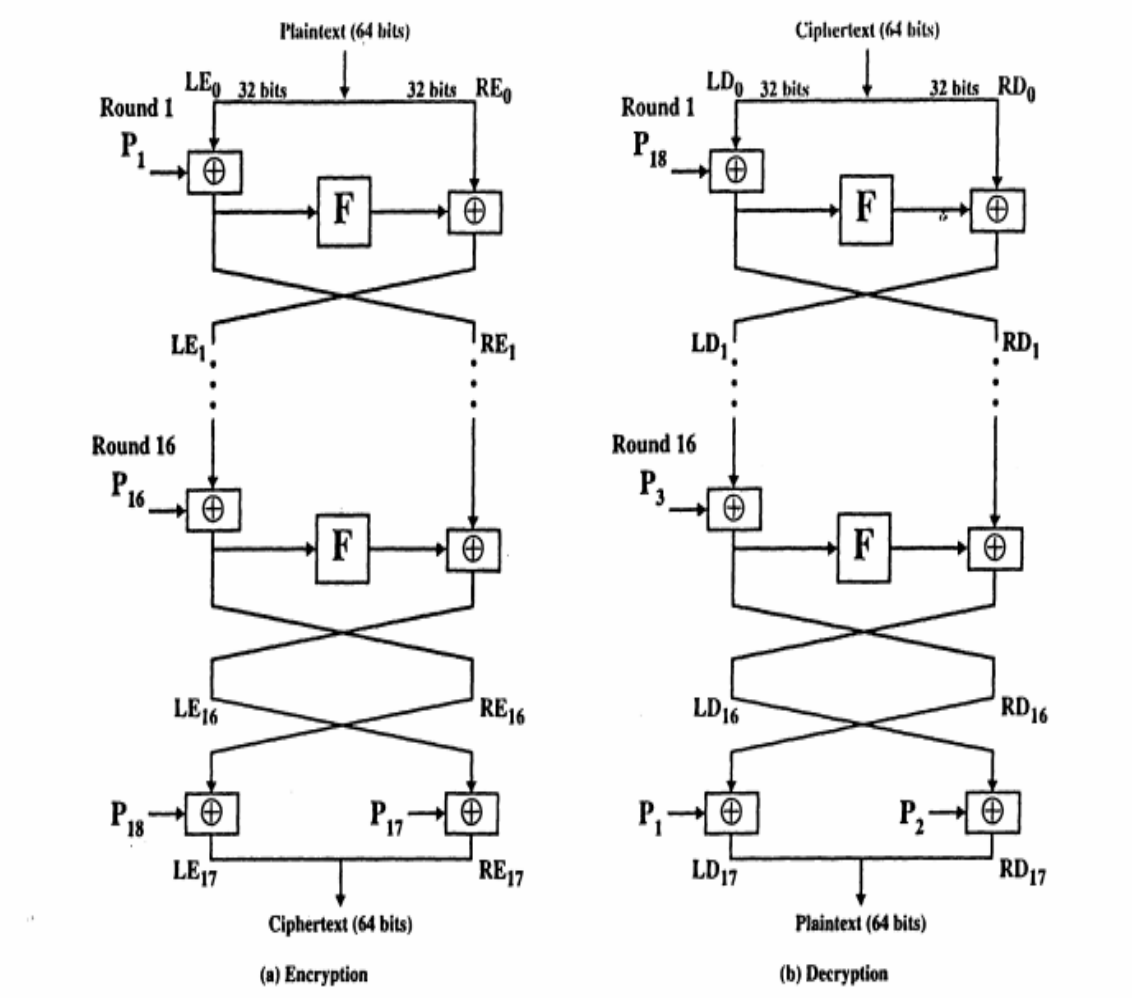

Figure 3. Blowfish Encryption and Decryption.

The Simulation by matlab:

m= secure IP Telephony

E= µ1üRÈ

D= secure IP Telephony

Elapsed time is 7.359 ms

2.3. INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)

IDEA algorithm consists of eight rounds followed by final transformation function and the algorithm divides the input into four 16 bit subblocks which called x1, x2, x3 and x4. Each of the rounds takes four 16-bit subblocks as input and produces 4 16bit as output blocks. The final transformation produces four 16 bit blocks which are concatenated to form the 64 bit ciphertext. Each of the rounds makes use of six 16 bit subkeys whereas the final transformation uses four subkeys for a total of 52 subkeys that it are all generated from the original 128 bit key.

For decryption algorithm: The decryption algorithm is the inverse process of the encryption algorithm which the decryption process is implementing by using the ciphertext as input to the same overall IDEA structure but with a different selection of subkeys.

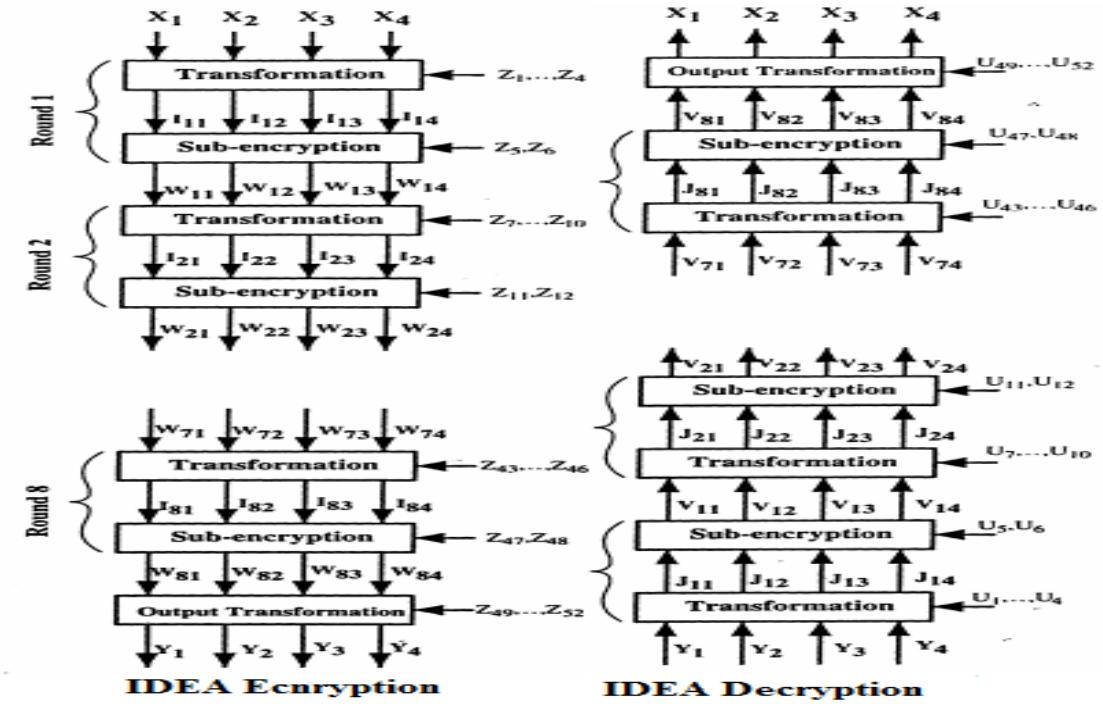

Figure 4. IDEA Encryption and Decryption

The simulation by matlab:
m= secure IP Telephony
E==½Ií ÈBa¾çü Èa2ìt
D= secure IP Telephony
Elapsed time is 8.609 ms

2.4 RIVEST CODES SCORECARD (RC5)

When we say w/r/b (32/12/16), this means 32 bit words (64 bit plaintext and ciphertext blocks), 12 rounds in the encryption and decryption algorithm, and the key length of 16 bytes (128bits).

LE(0) = A + S[0]
RE(0) = B + S[1]
LE(i) = ((LE(i-1) xor RE(i-1) <<<RE(i-1)) + S[2× i]
RE(i) = ((RE(i-1) xor LE(i) <<<LE(i)) + S[2×i +1]

For decryption, the 2w bits of ciphertext are initially assigned to the two one word variables LD(r) and RD(r)

RD(i-1) = ((RD(i) – S[2 × i+1] >>>LD(i)) xor LD(i))
LD(i-1) = ((LD(i) – S[2 × i] >>>RD(i-1)) xor RD(i-1)
A= RD(0) – S[1] B= LD(0) – S[0]

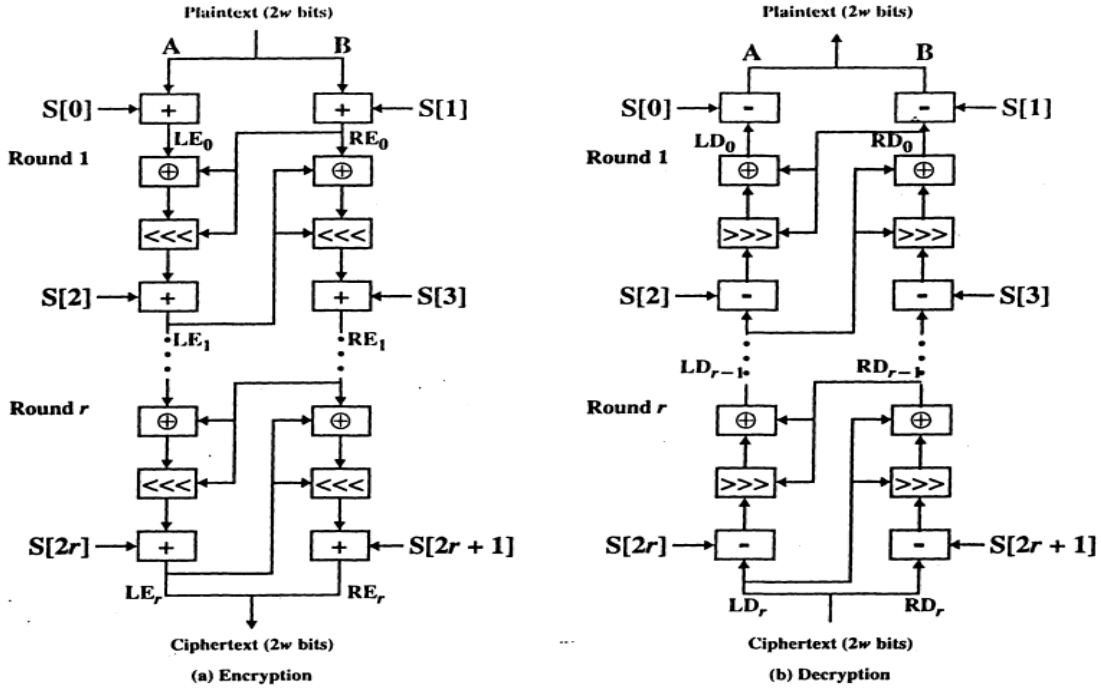

Figure 5. RC5 Encryption and Decryption.

The simulation by matlab:
m= secure IP Telephony
E==£ö DGB
D= secure IP Telephony
Elapsed time is 7.152 ms.

2.5 CARLISLE ADAMS AND STAFFORD TAVARES (CAST -128)

For encryption algorithm, the plain text is divided into two 32 halves L(0) and R(0) and the variables L(i) and R(i) to refer to the left and right half to the data after round (i) has complete. In the 16 round the output is swapped and the output is the concatenation of RE(16) and LE(16) which are used to the input for the decryption algorithm. And RE(16) and LE(16) are referred to the output of the encryption algorithm and also they are the input of the decryption algorithm after swapping.

L(0)‖ R(0) = plain text .
LE(i) = RE(i-1)
RE(i) = LE(i-1) xor Fi[R(i-1), Km(i), Kr(i)]
Ciphertext = RE(16)) ‖ LE(16)

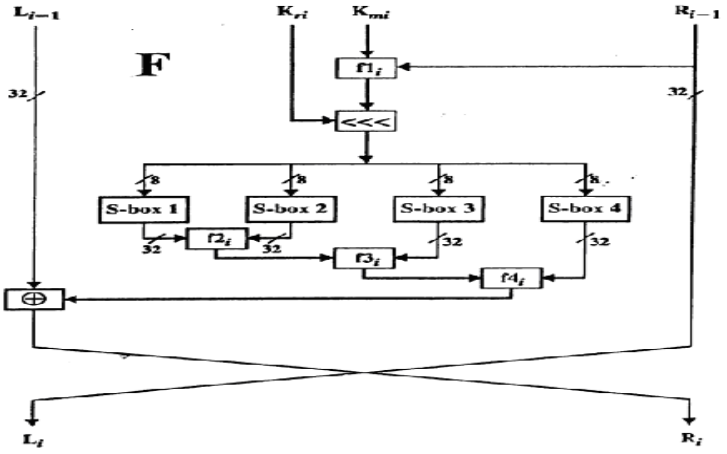

Figure 6. CAST-128 Encryption

But we achieved the simulation; in the round 1, 2, 14, 16 two but we noticed that there are long number of zeros of I so we use the padding operation for I .We noticed that some times the function is being negative value so it must be converted to positive value. All these notices will be happened according to type of voice file which converted to bits.
The decryption algorithm, we implement a novel decryption algorithm to get the original data. Because the encryption algorithm is very long and complicated so we modified and determined the decryption algorithm

The equation of decryption process as the following steps:
RD(i-1) = LD(i)
LD(i-1)= F((RD(i-1),km(i),kr(i)) xor RD(i)
(i) Will be decreased in the decryption algorithm for example:
RD(15) = LE16
LD(15)= F(RE(16),km(16),kr(16)) xor RE(16)
And so on

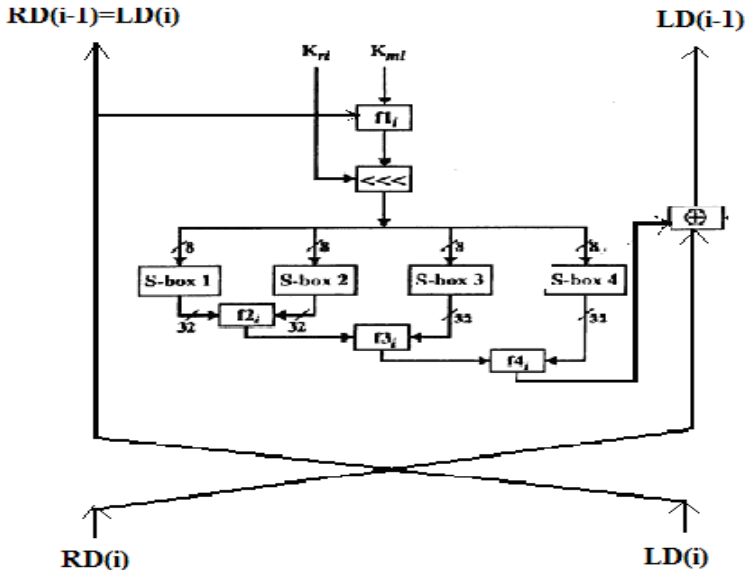

Figure 7. CAST-128 Decryption

The simulation by matlab:
mes = secure IP Telephony
E= êºÓ.n`Û
D= secure IP Telephony
Elapsed time is 42.057ms

2.6. TINY ENCRYPTION ALGORITM (TEA)

We use TEA algorithm but the processing time of the TEA algorithm is 200ms, so we modified TEA to implement SRTP with minimum time processing to take a less time. The maximum acceptable delay in packet delivery for optimal voice quality is 150ms, which can be extended up to 200ms. In our paper, we achieved the less time in encryption and decryption is 1.744 ms.
TEA advantages:

1. TEA is fast and most efficient cryptographic algorithm.
2. The using a Feistel cipher that it providing diffusion and confusion properties.
3. It saved 20 % of bandwidth and end to end delay.
4. Powerful algorithm which gives the best meets half way between security and efficiency.
   TEA emerges less attack than XTEA.

When we use number of round in TEA we notice that faster results but lower encryption quality and Encryption time is being linearly with number of rounds [19].

The TEA algorithm:

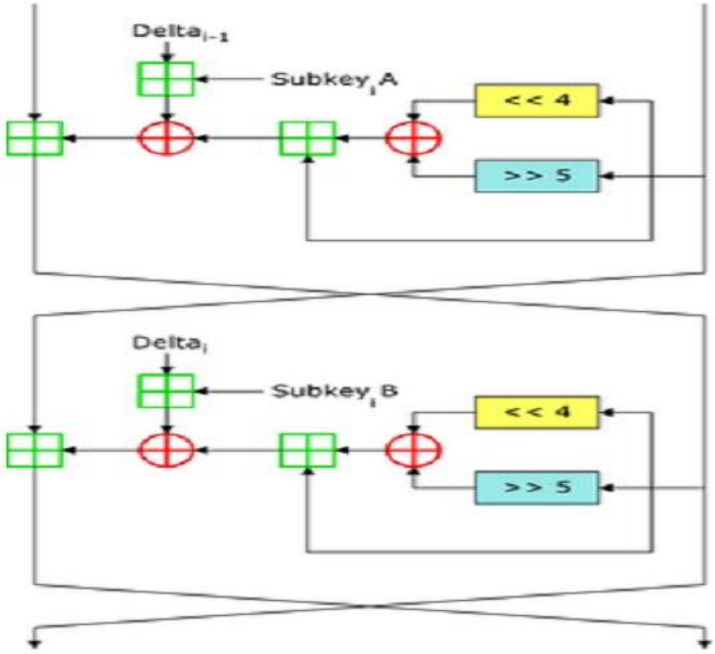

Figure 8. TEA Encryption

The Novel TEA Algorithm: We implement novel TEA encryption and decryption algorithm after our modification TEA algorithm to get less time.For encryption algorithm: we divided the plaintext into two parts (y and z) and used delta which identified 2654435769 or 9E3779B9. The K is gives the key of four words that defined (k0, k1, k2, k3) and n is the number of cycles which equal 16 cycles that use 32 Feistel rounds.The process:

1. Plaintext is divided into two parts right and left part (Y, Z).
2. The left part Z is shifted left by (4) and added to k0.
3. The Left part Z is added to the sum.
4. The left part Z is shifted right by (5) and added to k1.
5. Bitwise XOR the result of steps 2, 3 and 4.
6. The result of step 5 is added to the right part Y to produce Yi which swapped.
7. Yi is shifted left by (4) and added to k3.
8. Yi is added to sum.
9. Yi is shifted right by (5) and added to k4.
10. Bitwise XOR the result of steps 6, 7 and 8.
11. The result from step 10 is added to the left part Z to produce zi, and then swapped and so on.

The equation of novel TEA algorithm according to the figure:
z1= [(z<<<4) + k0] xor [z + sum] xor [(z>>>5) + k1]
yi = z1 + y
yi1= [(yi<<<4) + k2] xor [yi + sum] xor [(yi>>>5) + k2]
zi = yi1 + z

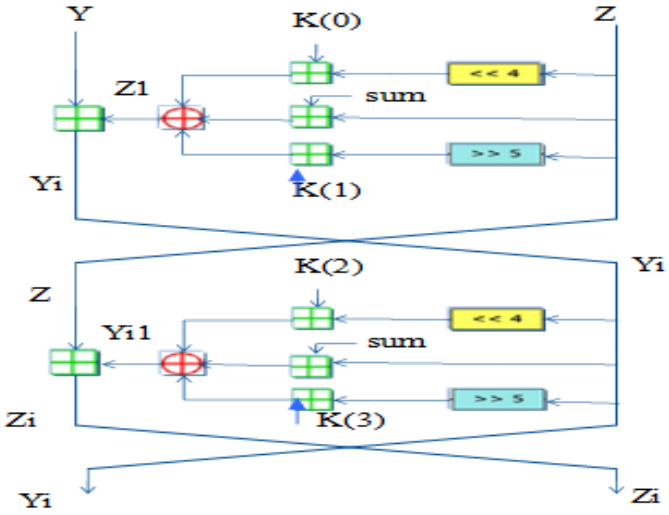

Figure 9. The novel TEA encryption

For decryption algorithm, It is the same way of the encryption but its inverse and sum= shift left of delta by 5. Note that: in the final decryption we use padding to produce the original message.
The equation of Tea decryption algorithm according to the figure:

y (i1)= [(y(i) <<< 4) + k2] xor [y(i) + sum] xor [y(i) >>> 5 + k3]
z(i-1) = yi1 + zi
zi1 = [(z(i-1) <<< 4) + k2] xor [z(i-1) + sum] xor [z(i-1) >>> 5 + k3]
y(i-1) = zi1 + y(i)

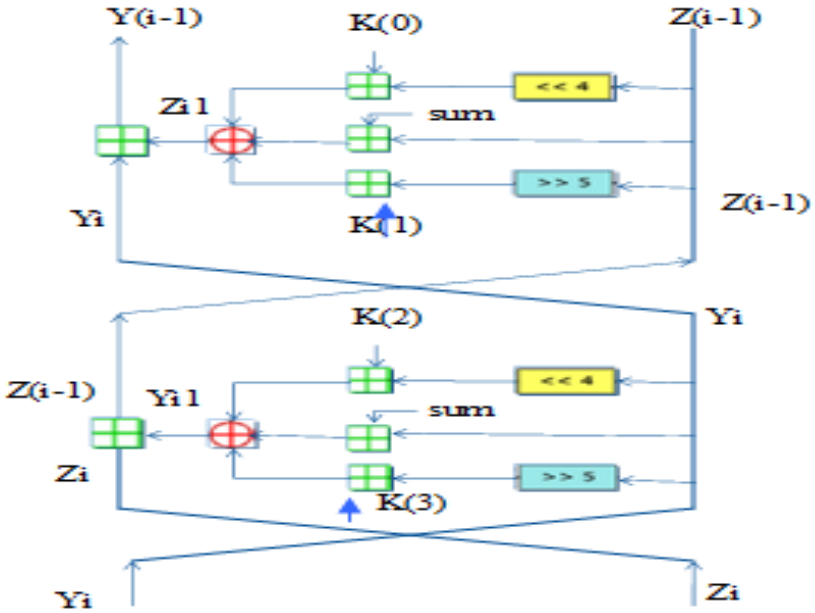

Figure 10. The novel TEA decryption

The simulation by matlab:
m = secure IP Telephony
E= ÒÝ2Aµ³PË
D= secure IP Telephony
Elapsed time is 1.744 ms.

3.7. FINAL RESULT

Table of Time of symmetric cryptographic algorithm shows the lowest time in the novel TEA algorithm after our medication of TEA and the highest time in the AES algorithm.

Algorithm Name	The Time
AES	92.06 ms
CAST-128	42.057 ms
Blowfish	7.359 ms
IDEA	8.609 ms
RC5	7.152 ms
The Novel TEA algorithm	1.744 ms

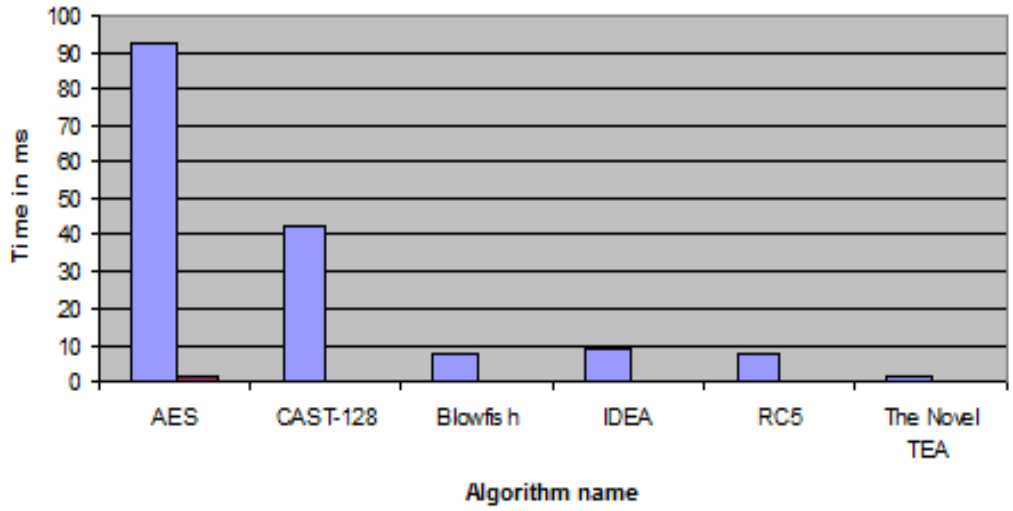

Figure 11. Throughput of each Symmetric Cryptographics Algorithm im mS

In Figure 10, we show the taking time of each encryption and decryption algorithm. The results show hat the novel TEA algorithm after our modification of TEA algorithm which takes less time than other algorithms and in addition to it is faster and saves bandwidth, end to end delay and powerful algorithm which gives the best meets half way between security and efficiency. It provides diffusion and confusion properties.

3. SRTP IMPLEMENTATION

3.1. KEY DERIVATION

The SRTP uses the maser key and the master salt which provided by an external key management protocol as input to PRF to derive a set of session keys which consisting of an SRTP encryption key, an SRTP salting key and an SRTP authentication key. For encryption, the SRTP are used to generate keystreams which are used for SRTP and SRTCP packets encryption and decryption algorithms [15].

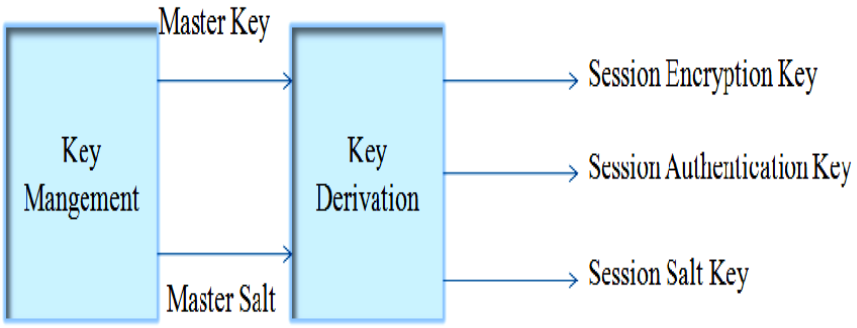

Figure 12. Key Derivation

For authentication, SRTP authentication keys are used to compute and prove the MAC of SRTP and SRTCP packets. The PRF is used for the session keys derivation that based on AES-CRT encryption algorithm. The master key is used as the AES encryption key and the initial value which generated using concatenation, shift and XOR operation. There are several families of KDFs, we use KDF in Feedback Mode and the output of the PRF is calculated by using the result of the previous iteration and, optionally using a counter as the iteration variable (s) [28].

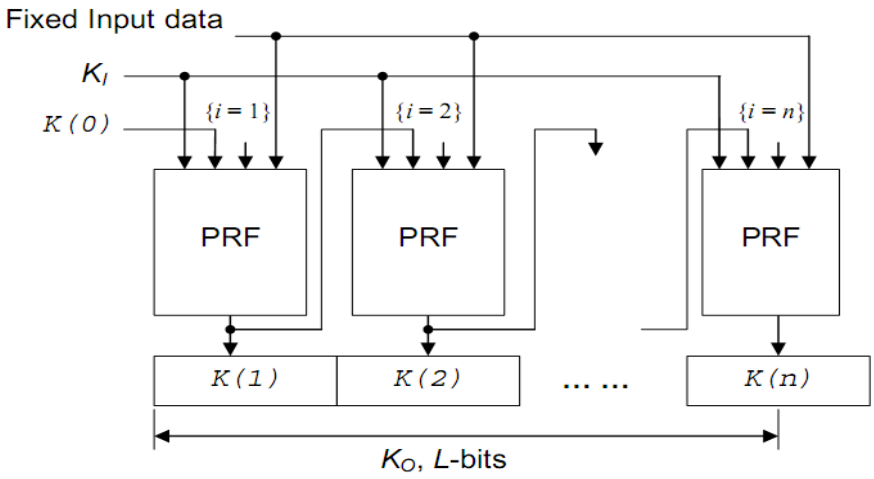

Figure 13. Key Derivation in Feedback Mode

mes = secure IP Telephony
Key = 1B01401291A97857A3BA5D63CB07D71D1B22EA1AFD918A1B5A64E94466 Elapsed time is 1.3772 ms.

3.2. ENCRYPTION ALGORITHM

In the sender the SRTP encryption and salt keys are used to generate the keystreams that used for the encryption and decryption SRTP packet. Encrypt the RTP payload to produce the encryption portion of the packet by using an encryption. We use novel TEA algorithm that we explain in section 2.6 which takes less time.

But we note that the time is changing according to the processor of the system.

3.3. AUTHENTICATION

Message authentication is the next process after the encryption process and protects the entire RTP packet by using session authentication key for the message authentication which is used to calculate and prove HMAC of the SRTP packets. The sender side computes authentication tag for authenticated portion of the packet. This step uses the current rollover, the authentication algorithm (SH1) and the session authentication key. The authentication tag is used to carry message authentication data. The authentication portion of SRTP packet consists of RTP header followed by the encrypted portion of RTP packet [13].

HMAC is used between two parties that share a secret key in order to authenticate information transmitted between these parties [13]. This standard defines a MAC that uses a cryptographic hash function in conjunction with a secret key; this mechanism is called HMAC and is a generalization of HMAC [13]. HMAC should be used in combination with an approved cryptographic hash function [13]. The hash function includes SH1 and MD5 but, we use SH1because the SH1 is more securing than the MD5.

HMAC(K) = Hash[(K xor opad) || Hash[(K+ xor ipad)||Message)]]
mes= secure IP Telephony
hash= 7BDDCBFD736363732
Elapsed time is 7.5343ms.

The SRTP receiver verifies message|| authentication tag pair by computing a new authentication tag over data using associated with the receives message if two tags are equal, then message || authentication tag pair is valid otherwise; it is invalid and error audit message "AUTHENTICATION FAILURE" must be returned.

hfirst= E0E4D8DC767970736064585C2024181C36363732
hash= 7BDDCBFD736363732
Elapsed time is 7.5343ms.

3.4. DECRYPTION ALGORITHM

In the Receiver side decrypt the encryption portion of the packet by using novel TEA algorithm in the section 2.6 (decryption algorithm) get the original data. The total processing time to implement SRTP in minimum time is 18.1548 ms including key derivation time, encryption time in the sender side, authentication time in the sender side, verification time of the receiver side and decryption time in the receiver side.

4. CONCLUSIONS

We selected six symmetric cryptographic algorithms (AES, Blowfish, IDEA, RC5, CAST-128, and TEA) and compared between them. AES algorithm is stronger than the other algorithm but it takes 92.06 ms. Blowfish algorithm has less power but more time, so the blowfish has disadvantages in the decryption algorithm over other algorithms in terms of time consumption and serially in the output. IDEA uses a 128 bit key that its length makes it impossible to break by simply trying every key . RC5 uses a pseudorandom initialization sequence followed by a complex set of operations involving variable length (rotations) and mod 2 additions, so it is difficult to say which of these approaches is superior and also for large key size, the security of RC5 strong. CAST-128, we implement the novel algorithm of decryption to get the original data. CATS-128 is complicated algorithm and takes 42.057ms to implement the encryption and decryption algorithm. TEA processing takes time 200 ms, so we need to modify TEA algorithm to produce a novel algorithm that it takes 1.744 ms. We select this novel TEA algorithm to implement encryption and decryption for SRTP implementation in minimum time that it is suitable for IP Telephony traffic.

We implemented SRTP by three phases; the first phase is the encryption process when we use the novel TEA algorithm (TEA encryption algorithm after our modification) which takes less time. After the first phase, the second phase is the Authentication process which authenticates the data by generating authentication tag and sends it to the receiver which it generating anther authentication to verify it. If two tags are equal, then it is valid, otherwise; it is invalid and error audit message "AUTHENTICATION FAILURE" must be returned. The third phase is the decryption process to get the original data by using novel TEA decryption algorithm.

Acknowledgment

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

REFERENCES

[1] Mihir Bellere's and Roch Guerin and Phollip Rogaway , IBM T.J.Walson Research Center , Dept. of Computer science university of California, XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions, 1995.
[2] Lecture 10: Message Authentication Code Yuan Xue, October 1995.
[3] H. M. Heys and S. E. Tavares, Department of Electrical and Computer Engineering Queen's University Kingston,

Ontario, Canada, On the Security of the CAST Encryption Algorithm.
[4] Xia Zhu, faculty of engineering and applied science mernorial University of Newfoundland, A New Class of Unbalanced CAST Ciphers and Its Security Analysis, April, 1997.
[5] C. Adams, Entrust Technologies Network Working Group RFC 2144, CAST-128 Encryption Algorithms may 1997.
[6] Ronald L. Rivest. MIT Laboratory for computer science 545 technology square, Cambridge, Mass. 02139, The RC5 Encryption Algorithm, March 20, 1997.
[7] Roger M, TEA Extensions, March 1997.
[8] William stallings, Cryptography and network security: principle and practice, Second edition, 1998.
[9] Burton S. Kaliski Jr. and Yiqun Lisa Yin, RSA Laboratories RSA Laboratories Technical Report TR-602 Version 1.0, Encryption Algorithm, September 1998.
[10] Roger M, TEA Extensions, March 1997.
[11] S´ ergio L. C. Salom˜ ao, Jo˜ ao M. S. de Alcˆ antara, Vladimir C. Alves and Felipe M. G. Franca, Military Institute of Engineering Pca. General Tiburcio 80, 22290-270 Rio de Janeiro, RJ, Brazil COPPE/Federal University of Rio de Janeiro, Improved IDEA, 2000.
[12] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001.
[13] Federal Information Processing Standards Publication 198, "The Keyed-Hash Message Authentication Code", March 2002.
[14] Lecture 11 Cryptography CS 555, Message Authentication Code, fall 2004.
[15] M. Baugher , D. McGrew Inc. M. Naslund E. Carrara K. Norrman Ericsson Research, Network Working Group Request for Comments: 3711 Category: Standards Track Cisco Systems, RFC3711 - The Secure Real-time Transport Protocol (SRTP), March 2004.
[16] How-Shen Chang, International Data Encryption Algorithm CS-627-1, Fall 2004.
[17] David A. McGrew and Scott R. Fluhrer Cisco Systems, Inc. multiple forgery attacks gainst Message Authentication Codes, May 31, 2005.
[18] Fourth Edition by William Stallings Lecture slides by Lawrie Brown (modified by Prof. M. Singhal, U of Kentucky), Chapter 11: Message Authentication and Hash Functions. 2005
[19] Ashraf D. Elbayoumy, Simon J. Shepherd Advanced Signals Laboratory School of Engineering Design & Technology University of Bradford, BD7 1DP, UK, A high grade secure VoIP using the TEA Encryption Algorithm, 2005.
[20] Simon Shepherd, Professor of Computational Mathematics Director of the Cryptography and Computer Security Laboratory, Bradford University, England, The Tiny Encryption Algorithm (TEA), 24 Feb 2006.
[21] NETWORK DESIGN SECURITY AND MANAGEMENT (IF452), May/Jun 2007.
[22] Ma Chunbo1, Ao Jun3 & Li Jianhua School of Information Security Engineering, Shanghai Jiaotong Univ., Shanghai 200030, P. R. China; The State Key Laboratory of Information Security, Beijing 100049, P. R. China; State Key Laboratory for Radar Signal Processing, Xidian Univ., Xi'an 710071, P. R. China, Broadcast group-oriented encryption secure against chosen ciphertext attack, Journal of Systems Engineering and Electronics Vol. 18, No. 4, 2007, pp.811, 2007.
[23] Nick Robinson, Origami kit for Dummies, 2008.
[24] Informational Report, Issue 1, CCSDS REPORT CONCERNING ENCRYPTION ALGORITHM TRADE SURVEY, ENCRYPTION ALGORITHM TRADE SURVEY, March 2008.
[25] Derek Williams CPSC 6128 – Network Security Columbus State University, the Tiny Encryption Algorithm (TEA), April 26, 2008.
[26] Uli Kretzschmar ECCN 5E002 TSPA – Technology / Software Publicly Available, AES128 – A C Implementation for Encryption and Decryption, Appli July 2009.
[27] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, International Journal of Computer Theory and Engineering, Vol. 1, No. 3, 1793-8201, Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types, August, 2009.
[28] Lily Chen, Computer Security Division Information Technology Laboratory C O M P U T E R S E C U R I T Y, US Department of Commerce Gary Locke, Secretary National Institute of Standards and Technology Patrick Gallagher, Deputy Director, NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, October 2009.
[29] Ozlem S¨onmez, Seminararbeit Ruhr-Universit¨at Bochum Chair for Communication Security Prof. Dr.-Ing. Christof Paar, Symmetric Key Management: Key Derivation and Key Wrap, November 2009.
[30] Dorgham Sisalem, John Floroiu, Jiri Kuthan, Ulrich Abend and HenninSchulzrinne, SIP SECURITY book by Wiley, 2009
[31] Nayantara Mallesh and Matthew Wright Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX, USA, The Reverse Statistical Disclosure Attack, 2010.
[32] Qutaiba Ali, Nada Abdul Ghani Computer Engineering Department, University of Mosul, Iraq, Reviewing Speaker

Recognition Influence in Strengthening VOIP Caller Authentication, February 17, 2010.
[33] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual
Kader, and Mohiy Mohamed Hadhoud (Corresponding author: Diaa Salama Abd Elminaam)Higher Technological Institute 10th of Ramadan City, Egypt Faculty of Computers and Information Minufiya University, Egypt, International Journal of Network Security, Vol.10, No.3, PP.216–222, Evaluating The Performance of Symmetric Encryption Algorithms, May 2010.
[34] Nick hoffman, A SIMPLIFIED IDEA ALGORITHM, 29 Apr 2011.

BIOGRAPHY OF AUTHORS

Samah Osamah M. Kamel Received the B.S. degree in electronics and communications from Zagazig Faculty of Engineering, Zagazig University, in 2001. Her research interests Secure IP Telephony Attack Sensor. She is a Network Engineer at computers & systems dept., Electronics Research Institute since 2002.

M. Saad El Sherif His M.Sc., and Ph.D. degrees from the electronics & communications dept. & computers dept., faculty of engineering, Cairo University, at 1978, and 1981, respectively. Dr. M. Saad El Sherif is a Prof., at computers & systems dept., Electronics Research Institute (ERI). He is supervising 3 Ph.D students, and 5 M.Sc. Students. Dr. M. Saad El Sherif had published more than 26 papers in communication and computer area. He is working in many communication and computer systems hot topics such as; A Novel Representation of Artificial Neural Networks with Dynamic, Automatic processing of bank checks Synapses, Improving the performance of random early detection algorithm forinteractive voice applications, Anew IP multicast QoS model forreal - time audio / vidio traffics on the IP based networks, Neural networks in forecasting models: nile river application and Anew internet videoconference transport protocol. Also he is a technical reviewer for many international journals. He is heading the Electronics Research Institute from 2009 to 2011.

Adly S. Tag Eldien Received the B.S. Degree in Electronics and communication, Benha University in 1984 and the M.Sc. in computer based speed control of single phase induction motor using three level PWM with harmonic elimination, Benha University, in 1989. The Ph.D. in optimal robot path control, Benha University, in 1993. He is currently an Association prof. in shoubra faculty of engineering and Manager of Benha university network and information center. And his research interests include Robotics, Networks, and Communication.

Sahr Abd El_Rahman Ismail Hassan, Her M.SC degree in in Electronics and communication, Benha University an an AI Technique Applied to Machine Aided Translation in 2003 and Phd. , Benha University in Reconstruction of High-Resolution Image from a Set of Low-Resolution Images in Jan 2008. She is PhD/ MSc Supervision in Secure IP Telephony Attack Sensors, Intelligent Zone Wireless Fire Alarm System and An Investigation & Reduction of PAPR in MIMO-OFDM Systems. She is Graduation Projects Supervision in Smart Home Automation with J2ME, Sentry Robot Navigation Using Internet Protocol, Store Humanized Robot Navigation, Touch Screen and Mobile Robot Guidance by Using GPS.