ENCRYPTION AND DECRYPTION

Samanvay Gupta*

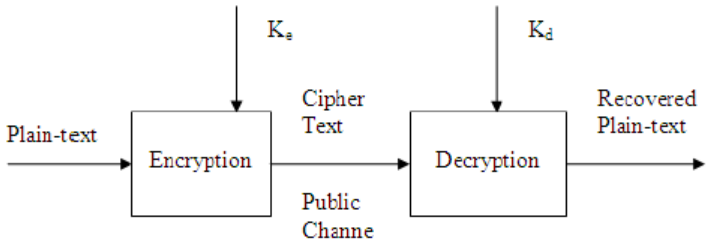
Abstract:

The encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) are widely used to solve the problem of communication over an insecure channel.Encryption is a well-established technology for protecting sensitive data. However, once encrypted, data can no longer be easily queried aside from exact matches [15], [16], [17]. This paper will present some basic knowledge on about importance of encryption, different types of encryption, VoIP encryption and image encryption. VoIP (voice over internet protocol) is a one of the best technology available for voice communication which has the potential to completely rework the world's cellular systems.

* 4th year 1st semester, Computer Science Department, Visvesvaraya College of Engineering & Technology.

Introduction

Encryption is used to protect the confidentiality of information when it must reside or be transmitted through otherwise unsafe environments. Encryption is also used for "digital signatures" to authenticate the origin of messages or data. Encryption algorithms themselves are rarely used alone in practice. Rather, they are typically embedded into a larger security system to ensure their correct and consistent use, since a failure to do can compromise the security of other messages, even those that have been properly encrypted.Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearranges the data bits in digital signals. In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies. This causes a battery gap [13, 14].



Encryption and Decryption procedure of a Cipher

History of Encryption

1.National Cryptologic Museum at National Security Agency (Ft Meade, MD)

2. World War II - breaking German and Japanese Codes

(a) WW II Codes and Ciphers - Colossus was the computer at Bletchley Park, England, which was built to break the German Enigma codes in World War II.

(b)Can Tab was a multi-processing Enigma emulator which worked in conjunction with Colossus: Colossus figured out how to set the Enigma rotors, then you went to the bombe to write out the decoded messages.

(c) Turing's Treatise on the Enigma

3. Modern encryption for privacy and authentication

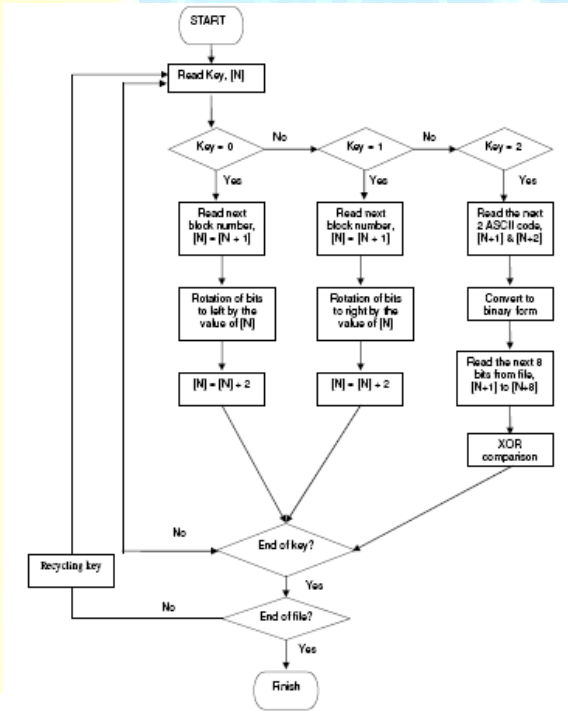
(a) History of Public-Key Encryption - explains how it works and how it came about. (Although this describes it as being invented in 1977, it had previously been invented at GCHQ in 1973, but kept secret.)

The Importance of Encryption

Encryption is one of the most important and most affordable defenses available to a small business.[2] If a hacker manages to get past all your other security measures, good encryption properly used will stop him in his tracks.If an identity thief manages to locate the records of your online credit card transactions, good encryption should protect you and your customers from a potentially debilitating crime.And if a laptop with sensitive information is stolen froman employee outside the office, good encryption will make that information completely unusable.Encryption has been used for thousands of years to protect information from prying

eyes, and even Julius Caesar was an avid user of codes during the Gallic Wars around 58BC to protect communications with his generals.In World War 2 the cracking of the encryption codes used in the German Enigma cipher machine helped the Allies achieve an important strategic advantage. And in the days leading up to the attack on Pearl Harbor the United States worked frantically to break the codes of the Japanese Purple encryption machine.Today encryption plays a crucial role in protecting our information, and most notably in securing our on-line purchases from attack. For the small business, encryption also plays an important role as a last line of defense against intruders and data thieves.By protecting important data (like credit card numbers) with encryption, intruders who manage to bypass all other security mechanisms will find encrypted information of little value.Properly encrypted data with well-protected keys will protect that data from being accessed and read. An intruder would have to either find or ‚Äòspoof‚Äô the key, guess it, or try every possible key combination until the right one is found.

Encryption flow chart:



Encryption Terminology

Encryption vs. Decryption- encryption means to encode or scramble, decryption means to decode or unscramble.

Cryptography vs. Cryptology. - Cryptography is the art or system of writing codes. Cryptology is the study of codes and code making systems.

Cipher vs. Cryptogram- the term cipher is used to both describe an encryption system or code, and a message that has been encrypted.

A cryptogram is a message hidden in a code. For example, an encrypted email could be considered a cryptogram.

Cryptanalysis - the science of cracking codes.

Network encryption (network layer or network level encryption)

Network encryption (sometimes called *network layer* or *network level encryption*) is a network security process that applies crypto services at the network transfer layer - above the data link level, but below the application level. The network transfer layers are layers 3 and 4 of the Open Systems Interconnection (OSI) reference model, the layers responsible for connectivity and routing between two end points. Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used. Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts. Network encryption is implemented through Internet Protocol Security (IPsec), a set of open Internet Engineering Task Force (IETF) standards that, used in conjunction, create a framework for private communication over IP networks. IPsec works through the network architecture, which means that end users and applications don't need to be altered in any way. Encrypted packets appears to be identical to unencrypted packets and is easily routed through any IP network. Network encryption products and services are offered by a number of companies, including Cisco, Motorola, and Oracle.

Popular Encryption Methods

DES the Data Encryption Standard has been in use for nearly thirty years, and despite many doubts about its true effectiveness the global banking community has relied on DES for decades to protect the daily financial transactions that we take for granted.

But DES is no longer regarded as sufficiently secure, and has been replaced by a number of more secure alternatives.

3DES Three-DES or Triple DES uses the basic DES algorithm, but encrypts data three times instead of once. It does offer significantly higher security than DES.

AES the Advanced Encryption Standard, or AES, was chosen by the NIST as the replacement for DES. After years of review and testing it is widely believed to be highly secure, and will remain that way for years to come.

Blowfish and Two fish both these algorithms were created by noted security expert Bruce Schneier and are widely used in commercial encryption products. Both are highly regarded, and while Blowfish provides a level of security adequate for data protection in a small business, Twofish provides considerably higher levels of security.

Block cipher

A block cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time. The main alternative method, used much less frequently, is called the stream cipher. So that identical blocks of text do not get encrypted the same way in a message (which might make it easier to decipher the cipher text), it is common to apply the cipher text from the previous encrypted block to the next block in a sequence. So that identical messages encrypted on the same day do not produce identical cipher text, an *initialization vector* derived from a *random number generator* is combined with the text in the first block and the key. This ensures that all subsequent blocks result in cipher text that doesn't match that of the first encrypting.

Escrowed Encryption Standard (EES)

The Escrowed Encryption Standard (EES) is a standard for encrypted communications that was approved by the U.S. Department of Commerce in 1994 and is better known by the name of an implementation called the Clipper chip. The significant feature of EES is its so-called key escrow method of enabling eavesdropping by authorized government agencies under certain circumstances. The encryption/decryption algorithm used by EES is called SKIPJACK. The feature can be incorporated into communications devices including voice, facsimile (fax), and

computer data. EES provides all the features of strong encryption with one exception: law-enforcement officials can intercept the communications given a court order allowing them to do so. This interception is made possible by means of a law-enforcement access field (LEAF), along with two decryption keys, one held by the National Institute of Standards and Technology (NIST) and the other held by Automated Systems Division of the Treasury Department.

Stream cipher

A stream cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. This method is not much used in modern cryptography. The main alternative method is the block cipher in which a key and algorithm are applied to blocks of data rather than individual bits in a stream.

Data Encryption Standard (DES)

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the sameprivate key.

DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession. This is not to say that a DES-encrypted message cannot be "broken." Early in 1997, Rivest-Shamir-Adleman, owners of another encryption approach, offered a $10,000 reward for breaking a DES message. A cooperative effort on the Internet of over 14,000 computer users trying out various keys finally deciphered the message, discovering the key after running through only 18 quadrillion of the 72 quadrillion possible keys! Few messages sent today with DES encryption are likely to be subject to this kind of code-breaking effort.

Uses of Encryption

Encryption can be used in several different ways as summarized below. In addition to the characteristics of a particular encryption algorithm that are required to support a given use, the

algorithm itself is generally integrated into a larger system that handles other aspects of the area to which encryption is being applied to ensure correct use and to minimize the visibility of the use of encryption. For example, if encryption is used for file protection, directories may also be protected and keys are managed on behalf of users so that normal file access does not change much.

Message Encryption This is the traditional use of cryptography. Blocks of text are encrypted as units. This is the normal way in which email is encrypted.

Digital Signatures Authenticating who sent a message is often useful. In the public key scheme, the secret decryption key can be used to encrypt, allowing the non-secret encryption key to be used to decrypt. Since only the secret key holder is presumed to have the secret key, only he could have encrypted/signed the message. Anyone can check the digital signature by applying the non-secret key. Secret, signed messages can be obtained by digitally signing with your secret key, then encrypting using the recipient's non-secret key.

Stream Encryption Some encryption schemes increase security by varying the key for separate packets of a long message. Often, the key is computed from previous packets. As long as all packets ultimately arrive, this works, but if packets are lost, subsequent packages are not decrypt able. Various synchronizations can be used to minimize the loss. This is particularly an issue for potential encryption of audio or video where the underlying transport will drop packets when load gets high.

File Encryption. Various encryption algorithms have been applied to files and databases. The main issue here is one of packaging the encryption naturally into normal file access and managing keys when a key may need to be used for a long time after it was originally used to encrypt.

Electronic Cash Cryptography is used to create unforgeable "electronic cash" tokens. Tokens include a serial number that can be decrypted (and saved) by the bank accepting the token. Reuse (illegitimate) of the token allows the user to be identified because the serial number will have already been seen in a previous transaction

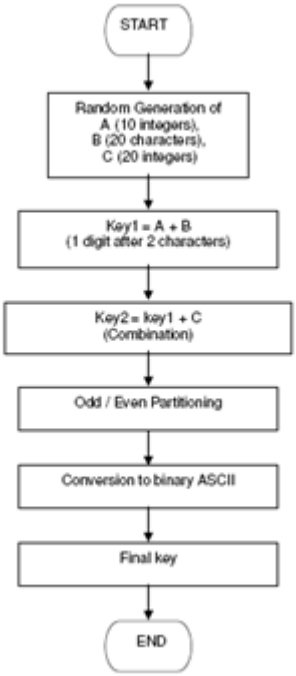
Encryption Strength

Encryption algorithms are generally rated by how much effort (time, processing power) is required to crack them based under a number of assumptions. These include amount of encrypted text available, whether the basic algorithm is known to the attacker, and whether encrypted text can be matched with its corresponding plaintext. In most cases, it is assumed that the attacker has access to all of these. In general, attacks can be made more time consuming by increasing key length. Generically, it is easy to increase key length as the attacker's power grows (due to faster computers); however, if the encryption is done in hardware this is not feasible. Even if this is possible, increasing key length requires that all users obtain new keys. The difficulties of key management are discussed below. Because given enough time a key will be discovered, the long term viability of an encryption requires that the key be changed periodically. The stronger the encryption, the less frequently keys must be changed to prevent attack. In general, because of increasing computing power, it is safest to assume that a message is not breakable only during a particular "time window" based on current and projected computing technology. Keeping messages secure for some time period is often sufficient because many messages are only important/embarrassing for a certain length of time. If perpetual security is required, there are theoretically unbreakable encryptions based on "one time keys" that are very secure but have enormous key management problems associated with them.

Key Management

To communicate, both sender and receiver need to share encryption/decryption keys (these may or may not be the same; see public vs. private). The dissemination of keys is of critical importance, since it is both cumbersome and a major source of vulnerability. There must be a way for a sender to let a receiver know the decryption key and to change that key as often as is dictated by the strength of the encryption (see tStrength). Key use must be synchronized so that both sender and receiver are using the same key for a communication. Messages intended for groups require the same key for all group members. Keys are also usually changed periodically in case the key was inadvertently divulged. This channel must be secure (private and verifiable), so that the key is not divulged in transit and so that it is possible to know that the key was obtained from the correct source to prevent "spoofing" (pretending to be someone else in order to steal a message by getting them to encrypt the message to you rather than the real recipient).

Couriers or complex protocols are used to exchange keys for private keys; public keys eliminate most key management problems. Figure shows the key management flow chart:



E-mail Encryption

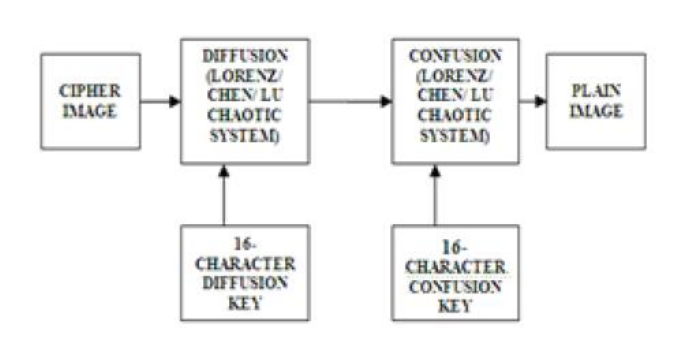
Today there are a lot of people acting as snoops. These people can take the form of hackers, private detectives, employees of various governments some being straight out and out dictatorships or monarchy run governments, kidnappers, ISP's, blackmailers and whomever. It seems that snooping has become a sport in a way. What we have done is establish a fewmethods for you to communicate with us securely. Securely means using serious encryption that would take decades to crack. Hush mail is a secure email provider. This means that when the email leaves your computer it is encrypted so anyone snooping on your email with packet sniffers or other methods will only get gibberish, nothing meaningful. The hush server delivers the mail. If the person has a hush mail account the message will automatically be unencrypted. If they have a regular email address the message will arrive unencrypted. This gives you a way to send us email including file attachments without exposing any private material. [1]

Proposed Cryptosystem

Encryption System

The proposed scheme is Different Chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted. Architecture of proposed Chaos based image cryptosystem. The first stage is the confusion stage and the second one is the diffusion stage. Among the three chaotic dynamic systems namely Lorenz, Chen and LU one is selected by the system parameter which is obtained from the key and it is applied to the digital color image encryption because of higher secrecy of high-dimension chaotic system. The second step of the encryption process is to encrypt the shuffled image by changing its pixel values based on one of the three high-dimensional chaotic systems (Lorenz, hen and LU). This is referred to as the diffusion stage. The initial conditions and the control parameters used to generate the chaos sequence in both the stages serve as the secret key in the two stages. The resulting image is the Cipher image. Separate key is used for permutation and diffusion stages of the encryption process to improve security of the algorithm.

Decryption System



The decryption system is illustrated in the Figure. The First stage in the decryption process is the diffused imaged encryption stage. In the encryption process, the pixel value diffusion was carried out with any one of the three chaotic systems. Therefore, in the decryption process to retrieve the original pixel values, again any one of the chaotic system (Lorenz, Chen, Lu) is employed in the first stage of decryption. The first stage of decryption process uses the three dimensional sequence generated by any one of the chaotic system .It is a kind of high-dimensional maps and complex enough the initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first stage. Second, in the encryption process, the pixel position permutation was carried out with any one of the chaotic system. The initial

conditions and control parameters for generating the chaos-sequence were used as the confusion key. Therefore in the decryption process, the same chaotic systems with same confusion key are used to get the original position of the image. The output of the decryption system gives the original image.

Encrypted IP Voice Call

VOIP works by converting analog voice signal into digitized data packets. The packets are sent out across the internet the same way as any other IP packets, using the internet's TCP/IP protocol The Internet is a notoriously insecure network. Anything send across internet can be easily snooped upon. This is of particular concern when highly confidential information, such as corporate data and credit card numbers, is transmitted across the Internet. Another related concern is that it can be difficult to know whether the person sending the information, is really who he says is he. Several ways have been developed to solve these problems. At the heart of them is Encryption, it is technique of altering information so to anyone other than the intended recipient it will look like meaningless garble. When the recipient gets the information, it needs to be decrypted that is, turned back into the original message by the recipient, and only by the recipient. In the Encrypted IP voice call this digitized voice data is transformed into Cipher text form using encryption techniques. Hence, the encrypted voice call is much secured as compared to VOIP.

Design encrypted IP Voice Call

Design specifies the logical structure of a research project and the plan will be followed in its execution. Suppose A want to communicate with B through secured voice communication. A and B must have android based mobile handsets with J2ME (proposed) application installed on it which is responsible for encrypted voice communication. [3], [6]

- The mobile handsets need to be registered at SIP server.
- When A calls B the application installed on mobile handsets will convert it into encrypted data.
- The encrypted data will travel through GPRS channels.
- The SIP server will route the call to the registered recipient B.

- The application installed on B handset will perform the decryption process.

Step 1: Voice communication can occur in 2 ways namely [5]:

- Wi-Fi (without the SIM card in Android handsets)
- GPRS (with SIM card in Android handsets). In the proposed work GPRS mode will be used.

Step 2: There would be 1 SIP server (Asterisk) and minimum 2 Android handsets. The handsets need to be registered at SIP server.

Step 3: The SIP server will be installed and configured on a system which will remain in an ON state and connected to the internet at all times.

Step 4: The Android application which will be developed needs to be installed on all the handsets which are registered in the SIP server and wish to communicate with each other using encrypted IP voice communication.

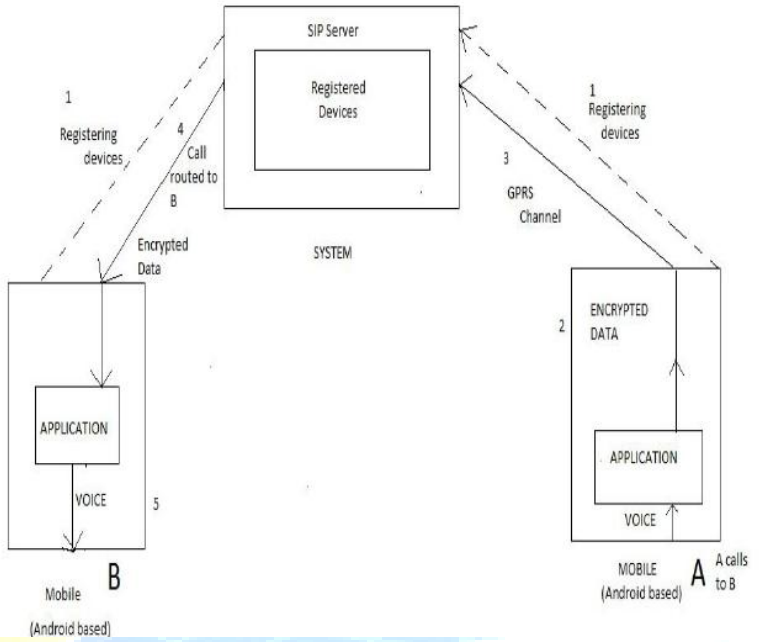
Step 5: The dialer will launch the Android application on his/her handset and dial the receiver's number. The dialing interface will be developed for the Android application. Once the call is made, the request will go the SIP server wherein the recipient's number will be checked and the call will be routed on its handset.

Step 6: Once the recipient receives the call through the same Android application and the dialer starts the conversation, all the digitized voice data will first be encrypted on the dialer's handset by the application and then sent to the SIP server for routing to the recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step 7: Once the recipient receives the call through the same Android application and the dialer starts the conversation, all the digitized voice data will first be encrypted on the dialer's handset by the application and then sent to the SIP server for routing to the recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step 8: The digitized voice data will travel in an encrypted fashion through the GPRS medium. The Android application will also have the capability that the recipient's may turn ON/OFF the decryption feature. That is to say, if the recipient turns ON the decryption feature, he will listen

to the original, decrypted voice. Else, the encrypted thing which could be a beep, non-understandable words, silence etc.



Steps for Encryption of Images

1- Sending the image to the function Encrypt which, in turn, sends the image to the function affine, which calls the procedure Keys to generate the randomly prime number between (1 256), under the condition that the common denominator between this number and 256 should be the integer one and keeping it in the matrix (A)

2- Storing seven random keys in a matrix.

3- Dividing the image into a set of blocks.

4- Encrypting each 7bits with the seven keys which stored in matrix (A), according to the following

Equation: $$\text{Cipher Bit} = (A * \text{plain Bit} + K) \bmod 226. \quad (7)$$

5- Repeating the step No. (4) in each 7 bits in the same block.

6- Repeating the steps No. (4) and (5) in all blocks

7- Resegmenting the image into whereas each block is a matrix of (4*4)

8- Substituting each block in the image by converting the row to the column.

9- Taking each 2 vertically adjacent bits from the bottom of the image (b1, b2)

10- Doing XOR between (b1 and b2) as: [8]

$$b = b1 \ XOR \ b2.$$

11- Doing XOR between the (b and 256) as: [9]

$$Cipher\ Bit = b \ XOR \ 256.$$

Steps for Decryption of Images

1- Taking each 2 vertically adjacent bits from the beginning of the image (b1, b2)

2- Doing XOR between (b1 and b2) as:

$$b = b1 \ XOR \ b2. \quad (10)$$

3- Doing XOR between the (b and 256) as:

$$Cipher\ Bit = b \ XOR \ 256. \quad (11)$$

4- Resegmenting the image into blocks each block is a matrix (4*4)

5- Doing the tract substitutes for each block in the image by converting the row to the column.

6- Taking the keys stored in the header of the image

7- Finding the inverse of each key from the keys stored in the inverse's matrix

8- Dividing the image into a set of blocks.

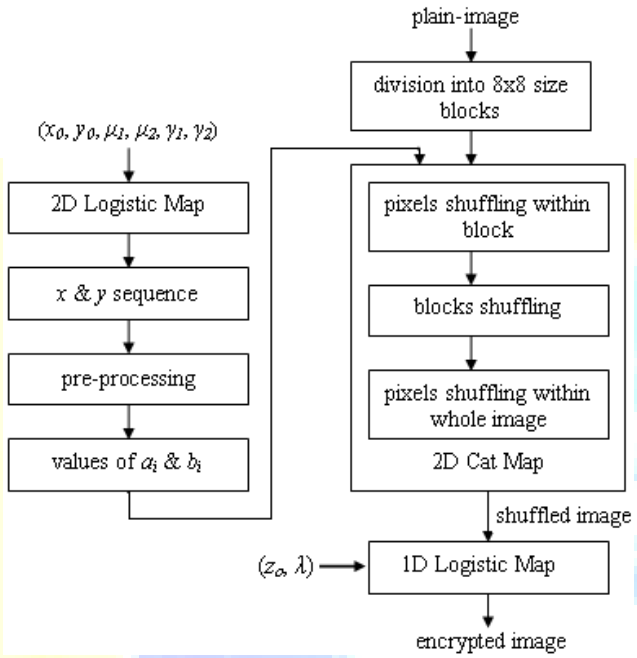
9- Decrypting each 7bits of the block accompanied with the inverse of the keys that stored in the matrix (A) according to the following equation:

$$Plain\ Bit = (A * (Plain\ Bit - K) mod\ 256. \quad (12)$$

10- Repeating the same step no. (9) for every 7 bits in the same block.

11- Repeating the steps No. (9) And (10) for all blocks.

The plain-image can be recovered successfully by applying the proposed algorithm in reverse order.



Original images

(a) **(b)**

Encrypted images

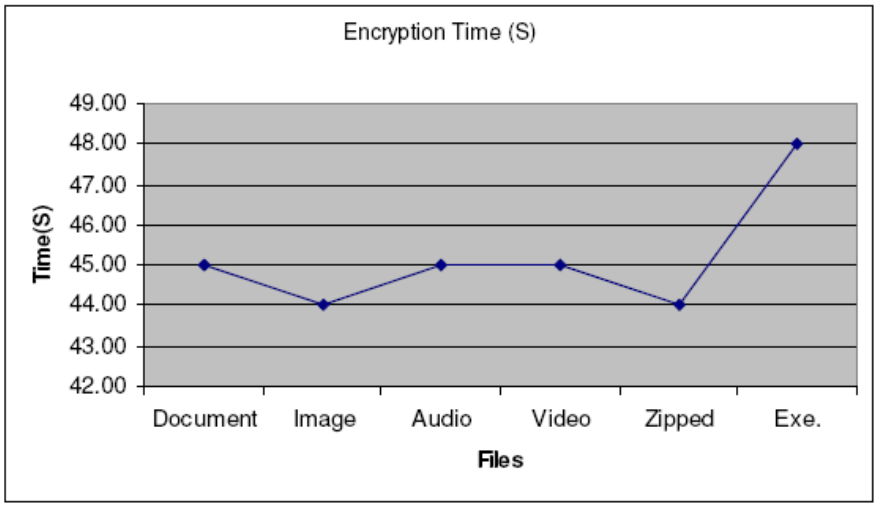
(a) **(b)**

Decrypted images

(a) **(b)**

Graphical view of the encryption time for different types of files and Success rate

File Types	File Size(Mb)	Encryption Time (S)	Success Rate
Document	1/ 3/ 5	9/27/45	100%
Image	1/ 3/ 5	10/26/44	100%
Audio/ Video	1/ 3/ 5	18/28/45	100%
Zipped	1/ 3/ 5	10/25/44	100%
Exe.	1/ 3/ 5	12/27/48	100%



Conclusion

The image and VoIP encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage and the secure VoIP calls. The encryption described in this paper might not be comparable to well-known encryption algorithms but its simplicity and availability proves the efficiency that fit the need and the requirement of security.

Reference

[1]http://www.lpoffshore.com/eng/encrypt.html

[2] http://education.identitytheftcouncil.org

[3]Ahmad Ali Habeeb, Mohammed A Qadeer and Shashir Ahmad (2007),"Voice communication over GGSN, SGSN, IEEE.

[4] Angelos D. Keromytis (2011)," A Comprehensive Survey of Voice over IP Security Research", IEEE

[5] Tuneesh, Lella and, Ricard (2007),''Privacy Of Encrypted Voice-Over-IP",IEEE

[6] Roy Chaoming Hsu, Cheng-Ting Liu, Wen-Ping Huang, Jun-Jay Yang, "An Embedded Software Approach for the Development of SIP-Based VoIP Server", Proceedings of the 11th Asia-Pacific Software Engineering Conference.

[7]BorkoFurht, EdinMuharemagic,DanielSocekMultimedia Encryption and Watermarking,Springer,USA.2005.

[8] Komal D. Patel, SonalBelani "Image Encryption Using Different Techniques: A Review" International Journal of Emerging Technology and Advanced Engineering. Volume 1, Issue 1, PP. 30 -34. 2011

[9]Monisha Sharma, ShriShankarcharya, ManojKumarKowar, "Image Encryption Techniques Using Chaotic Schemes: A Review" International Journal of Engineering Science and Technology.Vol. 2(6),PP. 2359-2363.2010.

[10] Nawal El-Fishawy, Osama M. Abu Zaid, " Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms " International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.

[11] IsmetOzturk, Ibrahim Sogukpınar, "Analysis and Comparison of Image Encryption Algorithms" World Academy of Science, Engineering and Technology 3,PP.26-30, 2005.

[12] Al-Ataby A. and Al-Naima F., "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform," The International ArabJournal of Information Technology, vol. 7, no. 4,pp. 358-364, 2010

[13] K. McKay, Trade-o®s between Energy and Security in Wireless Networks Thesis, Worcester Polytechnic Institute, Apr. 2005.

[14] A. A. Tamimi, Performance Analysis of Data Encryption Algorithms, Retrieved Oct. 1, 2008. (http://www.cs.wustl.edu/»jain/cse567-06/ftp/encryption perf/index.html).

[15] D. Denning. *Cryptography and Data Security*. Addison-Wesley, 1982

[16] B. Schneier. *Applied Cryptography*.JohnWiley, second edition, 1996

[17] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 2nd edition, 2002.