Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

Implementation and analysis of various symmetric cryptosystems

Himani Agrawal and Monisha Sharma

E & Tc. Department, SSCET, Bhilai-490020, Chhattisgarh India
himaniagrawaljka@gmail.com, monisha.sharma10@gmail.com

Abstract

This paper implements some of the widely used symmetric encryption techniques i.e. data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES), BLOWFISH and RC4 in MATLAB software. After the implementation, these techniques are compared on some points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, memory required for implementation and simulation time required for different message lengths.

Keywords: DES, 3DES, AES, blowfish, RC4, encryption, decryption, ciphertext, deciphertext, plaintext.

Introduction

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system such as a time sharing system. The need is even more acute for systems that can be accessed over a public telephone network, data network or the Internet. Implementation of digital security techniques becomes vital requirement especially for the transaction of secret information such as in military, forensic reports, for authentication of the firm. Nowadays these techniques are also used by the antisocial elements, terrorist to cause nuisances. Sometimes these nuisances take the form of unavoidable disaster, which echoes at international level (Schweighofer, 1997; Grover, 1998). Symmetric key cryptography is a form of encryption that uses the same key to both encrypt and decrypt data. The encryption algorithms are based on substitution and transposition techniques. Symmetric encryption employs two main methods to encrypt data: (a) Block cipher (Eg. DES, 3DES, AES & BLOWFISH) and (b) Stream cipher (Eg. RC4).

In order to use a block cipher, a specific size of data block is required. Stream cipher encrypts one bit or one byte of data at a time. In the article of RC4 from wikipedia, the application of RC4 in various fields is discussed. In cryptography, RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher and is used in popular protocols such as secure sockets layer (SSL) to protect Internet traffic and WEP to secure wireless networks. In article of AES from wikipedia, the symmetric cryptosystem AES is discussed in detail. In cryptography, the advanced encryption standard (AES) is an encryption standard adopted by the US government. As of 2009[update], AES is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information. In article secret-key cryptosystems (2009) various symmetric encryption techniques i.e. DES, 3DES, AES, BLOWFISH, IDEA, ONE TIME PAD, VERNAM CIPHER, HILL CIPHER etc. have been discussed. Schneier (1993) proposed Blowfish, a new secret-key block cipher. He also discussed the requirements for a standard encryption algorithm, while it may not be possible to satisfy all requirements with a single algorithm, it may be possible to satisfy them with a family of algorithms based on the same cryptographic principles. J.Frosen (1997. Practical cryptosystems and their strength) gave a brief view to many algorithms currently in use (eg. DES, 3DES, IDEA, 3IDEA & Skipjack) and gives somewhat more details on the most widely used cryptosystem (such as DES), also trying to predict their strength in the future applications. Practical cryptosystems include several algorithms, out of which many are currently used in applications. Some algorithms are more secure than others, while some have already been proved weak. The best applications combine different cryptosystems. After the extensive survey of the research papers it is observed that none of the research papers have discussed symmetric encryption techniques i.e. DES, 3DES, AES, Blowfish and RC4 all together with respect to the parameters i.e. Avalanche effect, memory required for implementation and simulation time. This thing gives a motivation to implement these techniques using MATLAB software and then discuss these techniques on the above specified points. This paper also discusses the applications of these techniques based on their strong and weak points.

Methodology

A brief description of the techniques implemented is as follows:

DES: It was created in 1972 by IBM using the data encryption algorithm and was adopted by the US government as standard encryption method for

Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

commercial and unclassified communications in 1977. DES begins the encryption process by using a 64-bit key. The NSA restricted the use of DES to a 56-bit key length, so DES discards 8-bits of the key and then uses the remaining key to encrypt data in 64-bit blocks. DES can operate in CBC, ECB, CFB and OFB modes, giving it flexibility. In 1998 the supercomputer DES cracker, assisted by 100,000 distributed PCs on the Internet, cracked DES in 22 h. The US government has not used DES since 1998.

3DES: DES was superseded by triple DES (3DES) in November 1998. 3DES is exactly what it is named-it performs 3 iterations of DES encryption on each block. It can do this in a number of ways, but the most common method is the Minus Encrypt-Decrypt-Encrypt (-EDE) method. Each iteration of 3DES using –EDE will encrypt a block using a 56-bit key. After encryption, use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key. Another method that can be used is Minus Encrypt-Encrypt-Encrypt (-EEE). This is three successive encryptions using a different 56-bit key. There are several keying methods that 3DES uses. All three keys can be independent of each other, or the first and third keys can be identical, with the second key being unique. All three keys can also be identical, which provides the least security, but is also the fastest to encrypt with. 3DES is still approved for use by US governmental systems, but has been replaced by the advanced encryption standard (AES) (Natural Science Report, 2006, Ochanomizu University, 57).

AES: AES was approved for use by the US government for the encryption of sensitive, but unclassified data in 2000. It was developed by two Belgian cryptographers, Joan and Vincent Rijmen, Rijndael is a portmanteau of the names of the two inventors. AES uses the Rijndael block cipher. Rijndael is a very resilient algorithm that has shown resistance to all known cryptographic attacks so far. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds. These round counts do not include an extra round of encipherment performed at the end.

Each processing round involves four steps: 1. Substitute bytes – Uses an S-box to perform a byte by byte substitution of the block, 2. Shift rows – A simple permutation, 3. Mix column – A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix and 4. Add round key – The key for the processing round is XORed with the data.

The algorithm itself is designed to exponentially increase the time it would take to mount a brute force attack on the cipher to several billion years (Natural Science Report, 2006, Ochanomizu University, 57).

Blowfish: It was developed by Bruce Schneier. It has a key length that can vary from 32 bits to a maximum of 448 bits (one to fourteen 32-bit words).That key is used to generate 18; 32 bit sub keys and four 8X 32 S-boxes containing a total of 1024 32-bit entries. The total is 4168 bytes. Blowfish is very fast since it encrypts data on 32-bit microprocessors at a rate of 18 clock cycles per byte, and can run in less than 5K of memory. The variable length key allows a tradeoff between speed and security. Blowfish is one of the most formidable conventional encryption algorithms. So far, the security of Blowfish is unchallenged (Schneier, *1993*).

The example of stream cipher is:

RC4: It is probably the best known symmetric encryption algorithm that uses a stream cipher. It is designed in 1987 by Ron Rivest for RSA security (Schneier, *1993*). RC4 keys can be anywhere from 1 to 2048 bits in length. These are used to initiate a 256-byte state table. This table is used by RC4 to generate a pseudo-random byte stream used to encrypt the plaintext. This stream is transformed with the plaintext data using an XOR (Exclusive or Boolean operator). The function will result in "True" only when a plaintext bit and its corresponding pseudo-random stream bit are opposite in value. In addition, every element in the state table is swapped at least once. This is what produces the cipher text.

Each of the above specified techniques is having their own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strong and weak points. Therefore the comparison of these techniques based on several features is necessary. Some of these points under which the cryptosystems can be compared are described below:

1. *Avalanche effect:* A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts.

2. *Memory required for implementation:* Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible.

3. *Simulation time:* The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.

Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

Results

The GUI (graphical user interface) version of the result is shown in Fig. 1. For preparing the GUI; static text, edit text and push button is used here. In one of the edit texts labeled as 'message'; the plaintext to be encrypted is typed. This plain text can be encrypted using any of the 5 methods implemented. On pushing the push button 'Encrypt ' encrypted text is displayed and on pushing the push button 'Decrypt ' decrypted text is displayed on the corresponding edit text box.

Analysis and discussion

All the above mentioned techniques i.e. DES, 3DES, AES, Blowfish and RC4 have been implemented in MATLAB 7.0 software (Advanced enryption standard**,** from Wikipedia, the free encyclopedia, (12th Jan 2010); Pratap, 2004; Stallings W (2004) Cryptography and network security, Pearson education; Secret-Key cryptosystems, 2009 (Symmetric Ciphers), SSH communications security). Based on the simulation results it is clear that the avalanche effect is highest in AES. It is medium in DES, 3DES and Blowfish. It is smallest in RC4. Therefore, if one desires a good avalanche effect; AES is the best option (Table 1).

From Table 2 it is clear that the memory required for implementation is smallest in RC4 whereas it is largest in 3DES. DES, AES and Blowfish require medium size of memory.

Fig. 1. GUI of symmetric encryption.

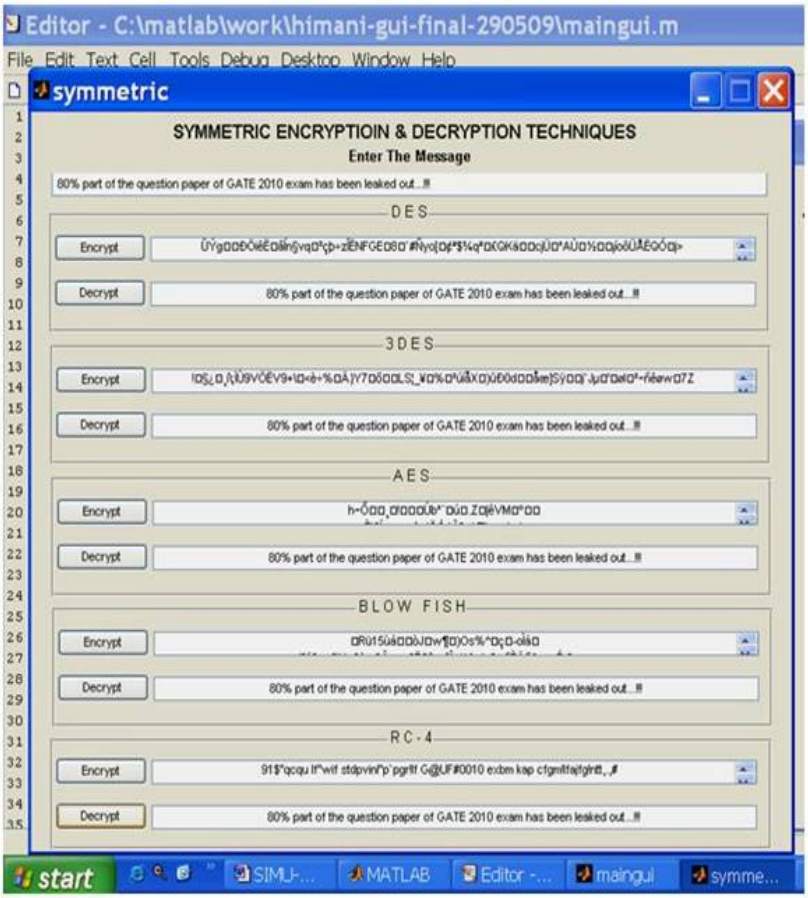

Table 1.Comparison based on Avalanche effect.

Technique	1 bit variation in key, keeping plaintext constant	1 bit variation in plaintext, keeping key constant
DES	30	34
3DES	37	33
AES	64	71
BLOWFISH	37	23
RC4	0	1

Table 2. Comparison based on memory required for implementation.

Technique	Memory required for implementation (KB)
DES	12.8
3DES	14.8
AES	10.6
BLOWFISH	6.88
RC4	2.49

Therefore, if the demand of any application is the smallest memory size; RC4 is the best option. From Table 3 the text files of different sizes/message lengths are taken. These are encrypted and decrypted using all the techniques one by one. The simulation time taken by different techniques is recorded in sec. It is clear that RC4 is the fastest technique. 3DES is the slowest technique. The speed of DES, AES and Blowfish is medium.

Table 3. Comparison based on simulation time required for different length of plaintexts (in sec.)
KEY: K1= 123456789012; K2= 923456789012.

Message length (KB)	DES (K1)	3DES (K1, K2)	AES (K1)	BLOWFI-SH (K1,K2)	RC4 (K1,K2)
0.013	0.3	0.63	2.46	3.98	0.19
0.636	4.80	15	4.86	5.12	0.20
2.90	57	292	12	9.32	0.79
6.17	245	1376	22.88	15.18	2.13
8.21	438	>2190	29.56	19.28	3.57

Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

Conclusion

1. DES is the most widely used encryption scheme, especially in financial applications.
2. In 3DES memory required for implementation is the highest means it is the slowest algorithm. This is the main drawback of 3DES. It is having a sufficient value of avalanche effect. Several internet-based applications have adopted triple DES. But because of various drawbacks it is not a reasonable candidate for long term use.
3. In AES the avalanche effect is highest. AES is being considered by the US government as a replacement for DES. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that are part of a game, or anything involving monetary transactions.
4. Blowfish is a very strong algorithm because of key dependent S-box design. In DES the design of S-boxes is fixed but in Blowfish the S-box design is key dependent. This featureb especially with larger S-boxes (e.g. 8 x 32)b yields highly non-linear results and therefore very difficult to cryptanalyse. In Blowfish each round consists of a key-dependent permutation, and a key- and data-dependent substitution therefore it is only suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. Blowfish is used in Secure Shell (SSH) technologies. It is used in a number of implementations, including the encryption of communications and HDTV transmissions.
5. RC4 is the shortest algorithm means it requires minimum memory space for implementation. RC4 is used in many commercial software packages such as Lotus notes and Oracle secure SQL. It is used in popular protocols such as Secure sockets layer (SSL) (to protect Internet traffic) and WEP

(to secure wireless networks). It requires the minimum simulation time. Each cryptosystems is having its own advantages and disadvantages.

References

1. Brian A. Carter, Ari Kassin and Tanja Magoc (2007) Symmetric cryptosystems and symmetric key management. *CiteSeerX*. 10.1.1.135.1231.
2. Grover D (1998) Forensic copyright protection. *The computer Law & Security Report*, 14, 121-122.
3. Pratap R (2004) Getting started with MATLAB, 6. Oxford University Press.
4. Schneier B *(1993)* Description of a new variable-length key, 64-bit block Cipher (Blowfish), Springer-Verlag, 191-204.
5. Schweighofer E (1997) Downloading information filtering and copyright. *Info. & Commun. Technol. Law*, 6 (2) 121-135.