Analysis of Cryptographic Algorithms

Kushal Patel[1] Sneha Shah[2]
[1]P. G. Student [2]Assistant Professor
[1, 2] Department of Electronics & Communication
[1, 2] L.J. Institute of Engineering and Technology, Ahmedabad, Gujarat, India

Abstract—Presently on a daily basis sharing the information over web is becoming a significant issue due to security problems. Thus lots of techniques are needed to protect the shared info in academic degree unsecured channel. The present work target cryptography to secure the data whereas causing inside the network. Encryption has come up as a solution, and plays an awfully necessary role in data security. This security mechanism uses some algorithms to scramble info into unclear text which can be exclusively being decrypted by party those possesses the associated key. This paper is expounded the varied forms of algorithmic rule for encryption & decryption: DES, AES, RSA, and Blowfish. It helps to hunt out the best algorithmic rule.

Key words: Cryptography, DES, AES, RSA, Blowfish

I. INTRODUCTION

Cryptography is an efficient method for shielding sensitive info .it is a technique for storing and sending knowledge in kind that solely those it's process for browse and process. For secure communication over public network knowledge may be protected by the method of encryption. Encryption converts that knowledge by any encryption algorithmic program using the 'key' in scrambled type. Solely user having access to the key will decipher the encrypted knowledge. Encryption may be an elementary tool for the protection of sensitive information. The aim to use encryption is privacy in communications. Here we tend to see the straightforward method of encryption & decryption.

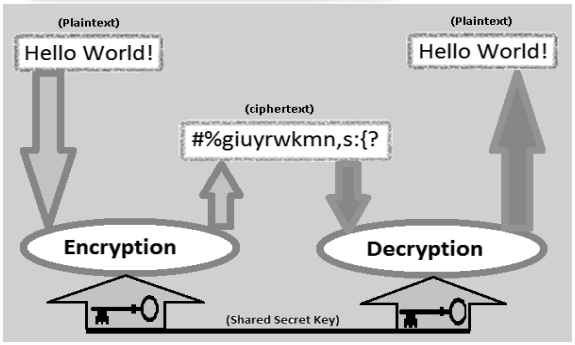

Fig. 1: Encryption & Decryption Process

II. DATA ENCRYPTION STANDARD (DES)

Data Encryption standard (DES) is designed and developed by IBM. It's published 1977 by National Institute of Standards and Technology as official standard for unclassified info. A lot of us government regulations refer for DES. Widely adopted by the trade to be used in security products. It may be simply implemented in hardware. Its high speed, up to gigabit/s with special chips. Data Encryption standard (DES) primarily adopted by business for security merchandise. Algorithmic program style for Encryption and decryption method has been finished same key. Data Encryption standard (DES) is a block cipher, with a 64-bit blocks size and a 56-bit keys. Data Encryption standard (DES) consists of a16-round series of substitution and permutation. In every spherical, knowledge and key bits square measure shifted, permutated, XORed, and sent through, 8 s-boxes, a group of search tables that square measure essential to the DES algorithmic rule. Decryption is basically a similar method, performed in reverse.

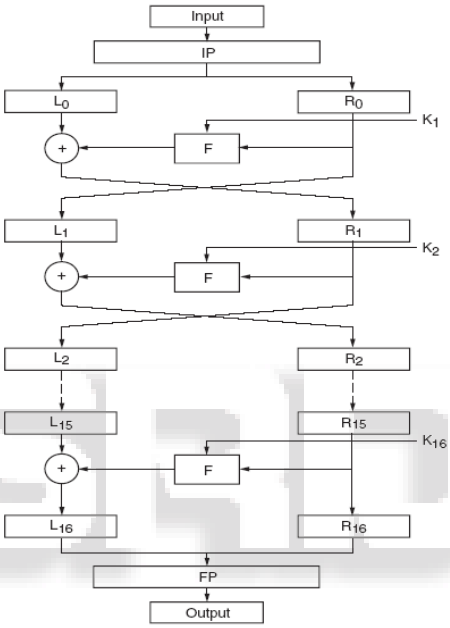

Fig. 2: Process of DES [11]

Here we see the figure for the process of DES.

The input block is 1st subject to an obvious permutation that within the customary is named the initial permutation. The permuted block is split into 2 equally sized blocks (L0, R0), that become the input for the primary round. The round manipulates these 2 blocks and also the output becomes 2 new blocks (L1, R1).

L1 = R0

R1 = L0 ⊕f (R0, K1)

The sub key K1 is chosen by a key planning algorithmic rule that generates sub keys from a56-bit long key. The DES contains sixteen rounds and every round may be represented as:

Ln = Rn-1
Rn = Ln-1 ⊕f (Rn-1, Kn)
Except within the last round, wherever the swap at the top of the round is skipped.
R16 = R15
L16 = L15 ⊕f (R15, K16)
The two blocks square measure finally subject to a final permutation, denoted FP, which is, in fact, the inverse of the Initial Permutation.

All rights reserved by www.ijsrd.com

III. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is published 1999 by Independent Dutch cryptographers. Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard re commended by NIST to replace DES. The Advanced encryption standard (AES) algorithmic rule is capable of using crypto graphical keys of 128, 192, and 256 bits to inscribe and rewrite information in blocks of 128 bits. As the AES algorithm may be used with three different key lengths, these three different ‘‘flavors’’ are generally referred to as ‘‘AES=>128’’, ‘‘AES=>192’’, and ‘‘AES=>256’’. AES uses several rounds in which each round is made of several stages. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. .it can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. To provide security AES uses kinds of transformation. Substitution permutation, combination and key adding every round of AES except the last uses the four transformations.

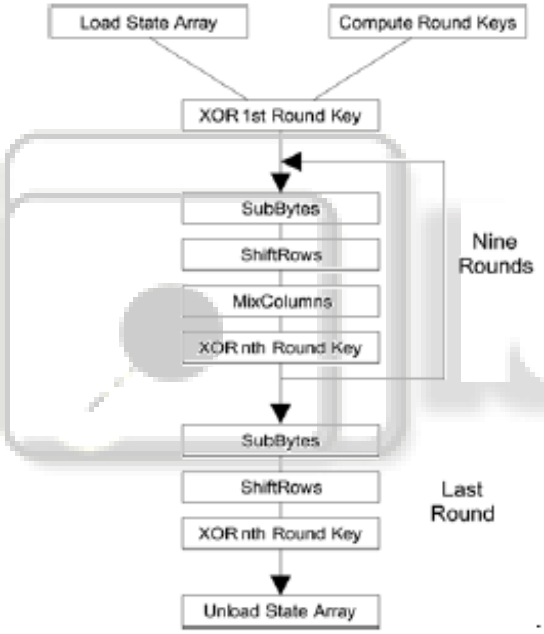

Fig. 3: Process of AES [2]

Sub Bytes: This operation may be an easy substitution that converts each bite into a unique value.

Shift Rows: every row is turned to the correct by a particular range of bytes

Mix Columns: Each column of the state array is processed singly to provide a brand new column. The new column replaces the previous one.

XorRoundKey: Adds the round key to the state using a bit-wise XOR operation.

Following process used to encrypt a 128-bit block:

1) Derive the set of round keys from the cipher key.
2) Initialize the state array with the block data (plaintext).
3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of state manipulation.
6) Copy the final state array out as the encrypted data

IV. RSA

RSA is a normally adopted public key cryptography algorithmic rule. The first, and still most ordinarily used asymmetric algorithmic rule RSA is known as for the 3 mathematicians who developed it, Rivest, Shamir, and Adleman. RSA nowadays is used in many software system merchandise and may be used for key exchange, digital signatures, or encryption of tiny blocks of information. RSA uses a variable size encryption block and a variable size key. The key combine comes from a really large number, n, that's the merchandise of 2 prime numbers chosen in keeping with special rules. Since it absolutely was introduced in 1977, RSA has been wide used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. within the authentication theme, the server implements public key authentication with consumer by signing a singular message from the consumer with its personal key, therefore making what's known as a digital signature. The signature is then come back to the consumer that verifies it using the server’s familiar public key.

Following steps are followed in RSA to get the general public and personal keys

1) Consider 2 giant prime numbers x and y such x~=y.
2) Compute n=x*y
3) Compute φ (xy) = (x-1)*(y-1)
4) Consider the general public key k1 such gcd (φ (n), k1) =1; 1 5.Select the personal key k2 such k2*k mod φ (n) =1

Encryption and Decryption are done as follow:

Encryption:
Calculate cipher text A from plaintext B such
$A=B^{k1} \bmod n$

Decryption:
$B=A^{k2} \bmod n=P^{k1\,k2} \bmod n$

V. BLOWFISH

Blowfish was designed in 1993 by Bruce Schneider as a quick various to existing encryption algorithms. Blowfish may be a symmetric key block cipher that uses a sixty four bit block size and variable key length. It takes a variable-length key from thirty two bits to 448 bits. Blowfish has variants of fourteen rounds or less. Blowfish is one in all the quickest block ciphers that has developed thus far. Slowness unbroken Blowfish from getting used in some applications. Blowfish was created to permit anyone to use encryption free of patents and copyrights. Blowfish has remained within the property right to the current day. No attack is understood to achieve success against it, although it suffers from weak keys problem .The Blowfish algorithm is for encryption. The encryption is a simply Feistal network of 16 rounds.

For the input of 64 bits, do:
Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
xL = xL XOR Pi
xR = F (xL) XOR xR
Swap xL and xR
Next i

All rights reserved by *www.ijsrd.com*

Swap xL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR Data

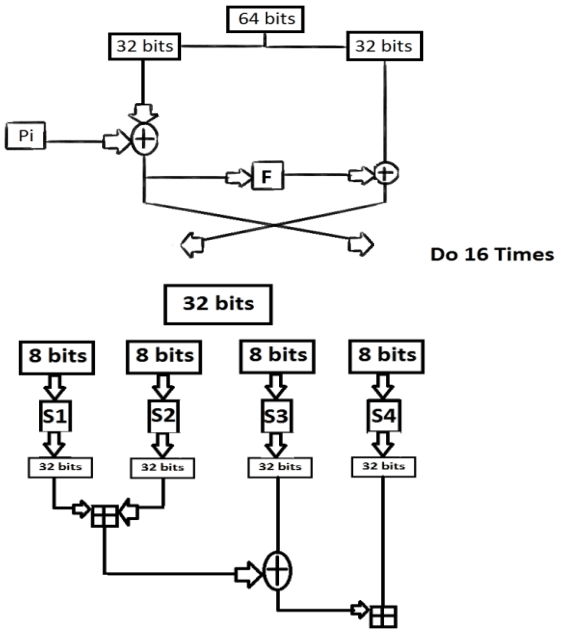

Fig. 4: Process of Blowfish [8]

The F function is: F (xL) = ((S1, a + S2, b mod 232) XOR S3, c) + S4, d mod 232 where a, b, c, d are four 8 bit quartered derived from xL.

VI. CONCLUSION

In Data communication, encryption algorithm plays an important role. My review work surveyed the existing encryption techniques like AES, DES and RSA, Blowfish algorithms. Based on the reviewed work, it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. I also observed that decryption of AES algorithm is better than other algorithms. Again from the reviewed stuff, I evaluated that AES algorithm is much better than DES, RSA & Blowfish algorithm.

REFERENCES

[1] Seyed Hossein Kamali, Reza Shakerian, Mohsen Rahmani, Maysam Hedayati, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption",*2010 International Conference on Electronics and Information Engineering (ICEIE 2010)*
[2] B. Padmavathi, S. RanjithaKumari "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", *International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064*
[3] Shashi Mehrotra Seth, Rajan Mishra ,"Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011 ISSN : 2229-4333(Print)|ISSN:0976-8491 (Online).
[4] Arjen K. Lenstra, "Unbelievable Security Matching AES security using public key Systems".
[5] Eman A. Abdel-Ghaffar, Mahmoud E. Allam, Hala A. K. Mansour, and M. A. Abo-Alsoud, "A Secure Face Recognition System",*978-1-4244-2116-9/08/$25.00 ©2008 IEEE*.
[6] Eustace Painkras, "Efficient Modeling and Implementation of Advanced Encryption Standard using S ystemC",*0-7803-8689-2/04/$20.00 Q2004 IEEE*.
[7] K. Guo, Y. Xue and C. Li, "An FPGA Implementation of the Advanced Encryption Standard with Composite Field S-box"
[8] Kevin Allison, Keith Feldman, Ethan Mick, "Blowfish"
[9] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994. B. Schneier, Description of a New Variable-Length Key, 64-BitBlock Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.
[10] Vikendra Singh, Sanjay Kumar Dubey, "Analysing space complexity of various encryption algorithms", ISSN 0976 – 6367(Print) ISSN 0976 – 6375(Online) Volume 4, Issue 1, January- February (2013), pp. 414-419
[11] Amit Dhir ,"Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs", *WP115 (v1.0) March 9, 2000*
[12] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei,NIEXuan, CAO Shui-ping,DAI Wei-di ,"Digital Image Encryption Algorithm Based on Chaos and Improved DES", *978-1-4244-2794-9/09/$25.00 ©2009 IEEE*.
[13] M. BrahmajiRao, "Classification of RSA and IDEA Ciphers".
[14] D. I. Manfred Lindner, Institute of Computer Technology-Vienna University of Technology.-Presentation.
[15] HuiQIN, TsutomuSASAO, Yukihiro IGUCHI, "A Design of AES Encryption Circuit with 128-bit Keys Using Look-Up Table Ring on FPGA", *IEICE TRANS.INF. &SYST.MARCH 2006.*
[16] Rashi Kohli, Manoj Kumar, "FPGA Implementation of Cryptographic Algorithms using Multi-Encryption Technique", International Journal of Advanced Research in Computer Science And Software Engineering.
[17] Abraham Panicker .O, A. Jabeena, Abdul Hassan Mujeeb, "Advanced Image Encryption and Decryption Using Sandwich Phase Diffuser and False Image Along with Crypto graphical Enhancement",978-1-4244-7286-4/10/$26.00 ©2010 IEEE.
[18] Yong Zhang, "Encryption Speed Improvement on an Improvement over an Image Encryption Method Based on Total Shuffling",*978-1-4673-6453-9/13/$31.00 ©2013 IEEE*.
[19] Swati Paliwal, Ravindra Gupta, "A Review of Some Popular Encryption Techniques"," International Journal of Advanced Research in Computer Science and Software Engineering.
[20] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "A Review and Comparative Study of Block based Symmetric Transformation Algorithm for Image Encryption", IJCTEE, Volume 1,Issue 2

All rights reserved by *www.ijsrd.com*