International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

Encryption And Decryption Using AES+BLOWFISH

Sahil Prakash, Shivam Prahlad Gupta, Pranjal Shrivastava

Department of Computer Science & Engineering, Krishna Engineering College, mohannagr,ghaziabad, Uttar Pradesh, INDIA

INTRODUCTION

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

Cryptography concerns

Attackers can bypass cryptography, hack into computers that are responsible for data encryption and decryption, and exploit weak implementations, such as the use of default keys. However, cryptography makes it harder for attackers to access messages and data protected by encryption algorithms.

Growing concerns about the processing power of quantum computing to break current cryptography encryption standards led the National Institute of Standards and Technology(NIST). to put out a call for papers among the mathematical and science community in 2016 for new public key cryptography standards. Unlike today's computer systems, quantum computing uses quantum bits (qubits) that can represent both 0s and 1s, and therefore perform two calculations at once. While a large-scale quantum computer may not be built in the next decade, the existing infrastructure requires standardization of publicly known and understood algorithms that offer a secure approach, according to NIST. The deadline for submissions was in November 2017, analysis of the proposals is expected to take three to five years.

AES (Advanced Encryption Standard)

AES Stand for the Advanced Encryption Standard it is used to protect electronic data by the help of cryptographic algorithm.

U.S government adopted the AES in 1977. It supersedes the Data Encryption Standard (DES).

The algorithm described by **AES** is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. NIST announced the AES in United States as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable.The Advanced Encryption Standard (AES) is defined in each of:

- FIPS PUB 197: Advanced Encryption Standard (AES)

- ISO/IEC 18033-3: Block ciphers.

BRIEF HISTORY OF AES ALGORITHM

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST) in 2000. The main aims of this algorithm was to replace DES algorithm after appearing some vulnerable aspects of it. NIST invited experts who work on encryption and data security all over the world to introduce an innovative block cipher algorithm to encrypt and decrypt data with powerful and complex structure. From around the world many groups submitted their algorithm. NIST accepted five algorithms for evaluate. After performing various criteria and security parameters, they selected one of the five encryption algorithm that proposed by two Belgian cryptographers Joan Daeman and Vincent Rijmen. The original name of AES algorithm is the Rijndel algorithm. However, this name has not become a popular name for this algorithm instead it is recognized as Advanced Encryption Standard (AES) algorithm around the world.

EVALUATION CRITERIA FOR AES ALGORITHM

Three important criterions were used by NIST to evaluate the algorithms that were submitted by cryptographer experts.

A. Security

One of the most crucial aspects that NIST was considered to choose algorithm it is security. The main reasons behind this was obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to other proposed algorithm. This wasachieved by doing a lot of testing on AES against theoretical and practical attacks

B. Cost

Another criterion that was emphasis by NIST to evaluate the algorithms it is cost. Again, the factors behind this measures was also clear due to another main purpose of AES algorithm was to improve the low performance of DES. AES was one of the algorithm which was nominated by NIST because it is able to have high computational efficiency and can be used in a wide range of applications especially in broadband links witha high speed.

C. Algorithm and Implementation Characteristics

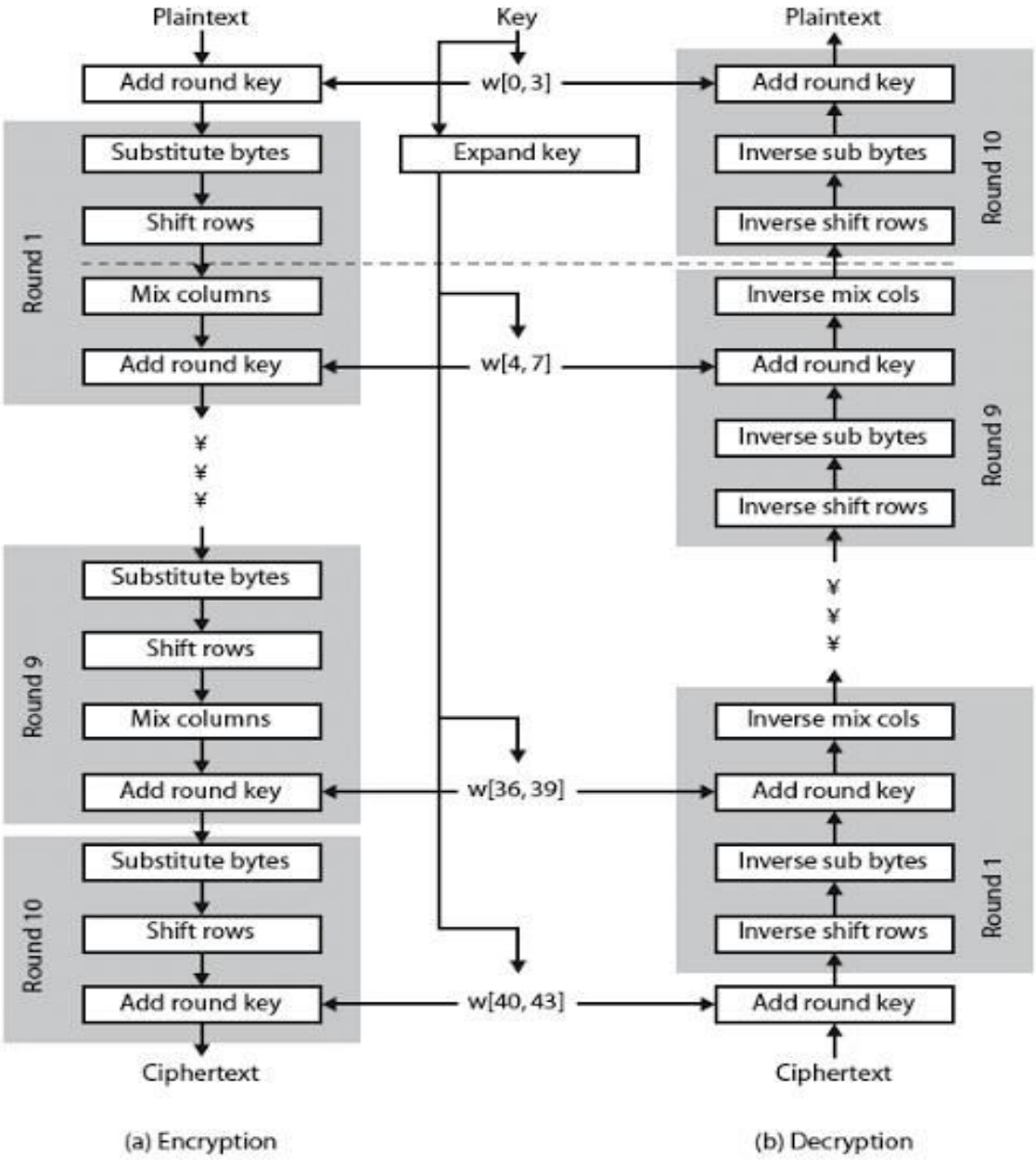
This criteria was very significant to estimate the algorithms that were received from cryptographer experts. Some important aspects were measured in this stage that is the flexibility, simplicity and suitability of the algorithm for diversity of hardware and software implementation.

BASIC STRUCTURE OF AES Algorithm

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms [7]. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

BLOWFISH ALGORITHM (BA)

Blowfish is designed in 1993 by Bruce



Schnier. Blowfish is a symmetric-key block cipher and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms.

BA is a symmetric block cipher that uses Feistel network, iterating simple encryption, and decryption functions of 16 times. Each Feistel structure offers various advantages, particularly in hardware. In the decryption process of the cipher
text, the only requirement is to reverse the key schedule. The
BA can be divided into key expansion and data encryption [1];
[12]; [29]. The key Expansion of BA begins with the P-array and S- boxes with the utilization of many sub-keys, which requires Precomputation before data encryption or decryption. The P- array comprises eighteen 32-bit sub-keys: P1, P2… P18. In this section a maximum key of 448 bits is converted
into several sub-key arrays of up to a total of 4168 bytes.

There are 256 entries for each of the four 32-bit S-boxes:
S1,0, S1,1,..., S1,255
S2,0, S2,1,..., S2,255
S3,0, S3,1,..., S3,255
S4,0, S4,1,..., S4,255

Below is the explanation of how these sub-keys are calculated:-

1. First, the P-array is initialized followed by the four S- boxes with a fixed string which has the hexadecimal digits of pi.
2. XOR P1 with the key's first 32 bits, XOR P2 with its second 32 bits, and so on until the key's bits are up to P14. The cycle is iterated through the key bits until the entire P-array has been XOR-ed with key bits.
3. The BA is then used for encrypting the all-zero string employing the described sub-keys in steps 1 and 2.
4. P1 and P2 are replaced with the step 3 output.
5. Encrypt the output of step 3 with the BA using the sub-keys that have been modified.
6. Output of step 5 is used to replace P3 and P4.
7. The process is continued, and all elements of the P- array are replaced, followed by all four S-Boxes, with
the output continuously changing.

PRODUCTS THAT USE BLOWFISH

Though it is not as secure as other symmetric encryption algorithms, many products in many different areas of the Internet utilize Blowfish. Different types of products that Blowfish is a part of are:

- **Password Management**: Password management software and systems protect and create passwords. Blowfish has been used in a variety of password management tools to both create passwords and encrypt saved passwords. Examples of password management tools using Blowfish include:
    - Access Manager
    - Java Password Safe
    - Web Confidential

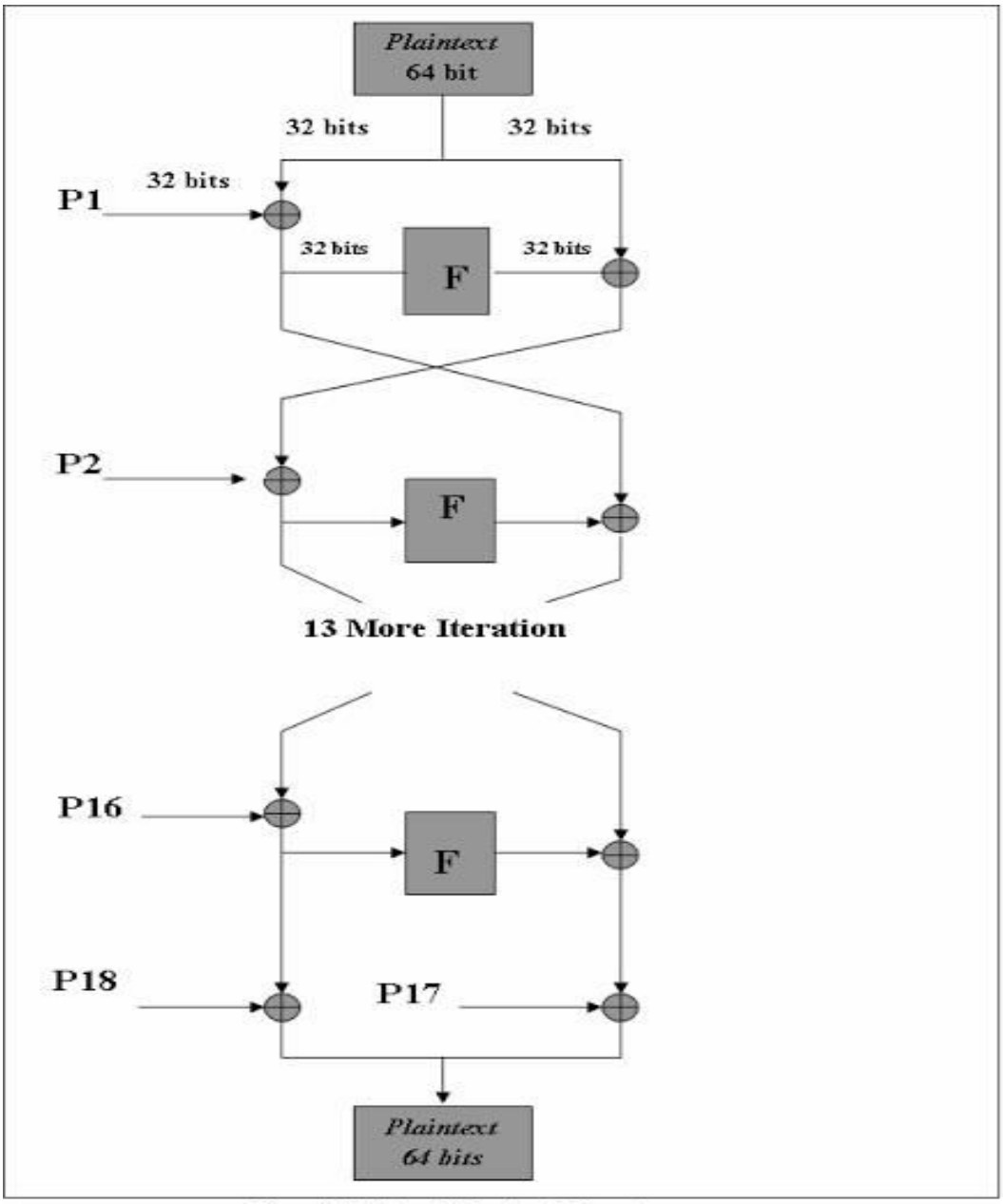


Fig. (1) Blowfish Architecture

- **File/Disk Encryption**: Software that encrypts files or disks is extremely common today as so many organizations have sensitive data they need to keep secure. This software must be straightforward for use by companies and quick to finish the encryption process. Thus, Blowfish is utilized in these encryption systems often in products such as:
    - GnuPG
    - Bcrypt
    - CryptoForge

- **Backup Tools**: Software that backs up vital infrastructure in an organization must have the ability to encrypt information in those backups. This is in case the backup contains sensitive information. Backup systems that use Blowfish are:
    - Symantec NetBackup
    - Backup for Workgroups
- **Email Encryption**: Encryption for emails is extremely important on any device. Different IOS, Linux, and Windows software all use Blowfish for email encryption. Examples:
    - A-Lock
    - SecuMail
- **Operating System Examples**:
    - Linux
    - OpenBSD
- **Secure Shell (SSH)**: Secure Shell is used to remotely access computer networks while authenticating the user through the use of encryption methods like Blowfish. Examples:
    - OpenSSH
    - PuTTY

PROPOSAL :

A novel and highly secure encryption methodology using a combination of AES and blowfishl crypto.

With the ever increasing human dependency on The Internet for performing various activities such as banking, shopping or transferring money, there equally exists a need for safe and secure transactions. This need automatically translates to the requirement of increased network security and better and fast encryption algorithms. This paper addresses the above issue by introducing a novel methodology by utilizing the AES method of encryption and also further enhances the same with the help of blowfish cryptography.

In this method the secret message is divided into two parts after which the message the first stage of the encryption message is encrypted using AES and the second stage i.e. the decryptione is done using the blowfish technique.

Modules

- Encrypt: Here the message to be sent has to go through 2 stages of cryptography . 1st stage is of encryption of the message which is encrypted using AES and the cipher text is sent forward.
- Decryption- Here the second stage is of decryption of message which is performed using the Blowfish technique.

Advantages

- This system provides high level of security as the message is now shielded with 2 layers of security.
- It is a novel and combinational approach of two secure techniques. Hence it will not be easy to crack by attackers.

Application

This application is useful in sensitive information. For example any company important message.

SUMMARY :

This research proposes an improved algorithm for the implemented asymmetric AES and blowfish cryptographic encryption/decryption algorithm in a wireless communication system and evaluated text message transmission performance of the results obtained in the present simulation study, it can be concluded that the deployment of AES and Blowfish cryptographic algorithm in wireless communication system is very much effective in proper retrieval of transmitted text message at the receiver end.