Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks

Archisman Ghosh

Department of Computer Science & Engineering, National Institute of Technology, Durgapur, West Bengal, India

---

Abstract - *Encryption is the process of encoding data to prevent unauthorized access. Cyber security is the need of the hour which ensures transfer of data across the internet with confidentiality and integrity, and provides protection against malicious attacks. In this research paper, comparison between the encryption algorithms, viz. AES (Advanced Encryption Standard), Blowfish, and Twofish is done in terms of time of encryption and decryption, and their throughput, and the results are analysed indicating the superiority of Twofish over AES and Blowfish as a viable algorithm for data encryption in wireless networks.*

Keywords: Cryptography, Network security, AES, Blowfish, Twofish, Secure communication.

1. Introduction

Owing to the advancement in internet accessibility and networking, most of the security sensitive stuff like internet banking, online shopping and bill payments is done through wireless networks. Therefore, such transactions demand to be end-to-end encrypted and should be purely private so as to ensure data confidentiality, integrity and availability, also known as the CIA triad [1].

In order to increase the efficiency of implementation of data security according to the CIA triad, the algorithms (like DES, 3DES, AES, RSA, Blowfish,Twofish) should be used alongside Hash-based Message Authentication Code (HMAC) for authentication purposes to ensure a safe WiFi design [2].

The process of encryption translates the data to a code to ensure the security of the data. Encryption algorithms perform various substitutions and transformations on the plaintext (original message before encryption) and transforms it into ciphertext (scrambled message after encryption). These are classified into two groups: Symmetric Key (also known as secret-key) and Asymmetric Key (also known as public-key) encryption [3].

A secure WiFi system uses algorithms such as DES, RSA, AES, Blowfish and Twofish to secure the communication over seemingly unsecured Internet channels. In addition, the existing cryptographic algorithm is based on an encryption model designed by Horst Feistel of IBM [4].

In this paper, a comparative study of the cryptographic algorithms: AES, Blowfish and Twofish has been done and the results have been analysed in order to find the algorithm most suitable for encrypting data in wireless networks.

2. Overview of the algorithms

2.1 AES

The Advanced Encryption Standard (AES) is a cryptographic algorithm for encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) [5]. NIST selected different key sizes of 128, 192 or 256 bits for which there would be 10, 12 or 14 rounds of encryption respectively to encrypt a block of 128 bit plaintext to a 128 bit ciphertext or decrypt a block of 128 bit ciphertext to a 128 bit plaintext. It is the successor to the DES which was published in 1977 [6]. It follows an algorithm which is symmetric-key in nature.

AES operates on a 4 by 4 column-major order matrix of 8-bit bytes which is known as the State array which is modified at each stage of encryption. In the first *N-1* (*N* depends on the length of the key used for encryption) rounds the matrix undergoes 4 different transformation functions, viz. SubBytes, ShiftRows, MixColumns and AddRoundKey. The matrix undergoes an AddRoundKey function before being entered in the rounds and the last round has only three transformation functions. The Key expansion function generates *N+1* round keys, each of which is a distinct 4 by 4 column-major order matrix. Each round key serves as one of the inputs to the AddRoundKey transformation in each round [3].

The SubBytes step involves the replacement of each byte of the State array with a SubByte using a 8-bit substitution box (the S-box). The S-box is derived from the multiplicative inverse over Galois Field of GF (2^8) in order to make the cipher non-linear [7]. In the ShiftRows step the first row of the State array is kept unchanged and the

bytes of the following rows are shifted by offsets of 1, 2 and 3 respectively. In the MixColumns function the four bytes of each column of the State array are combined using linear transformation using 8-bit bytes as the coefficients of a polynomial of order x^7[3]. In the final AddRoundKey step the State array is combined with the subkey generated by a main key. The combination is done by performing XOR between every byte of the subkey and the State array [8].

2.2 Blowfish

Bruce Schneier designed the Blowfish algorithm to be a symmetric-key block cipher in 1993. A few of the striking features of the Blowfish algorithm are the complicated key schedule and the key-dependant substitution boxes [9].

The algorithm has a block size of 64 bits and the key size ranging from 32 to 448 bits [9]. It is a 16-round Feistel Cipher with subkey-arrays, viz. the P-array and the 4 S-boxes. Each round of the Blowfish algorithm undergoes four steps. In the *nth* round, the left part of the block is XORed with the *nth* P-array followed by inputting it in the F function of the Blowfish algorithm. The output of the F function is XORed with the right half of the initial block and then swapped [9].

2.3 Twofish

When NIST called for a block cipher, Twofish was submitted alongside AES and it went on to be one of the finalists of the contest but was never considered for standardization.

The building blocks of Twofish are 16 rounds of Feistel networks, four different key-dependent 8 by 8 bit S-boxes, Maximum Distance Separable (MDS) matrices, and the idea of key whitening and key scheduling. The design parameters include a 128-bit symmetric block cipher, key lengths of 128, 192 and 256 bits, and the absence of weak keys.

Twofish was designed based on simplicity of the algorithm. However, the performance of Twofish is heavily dependent on hardware (in terms of the power of CPU and/or the VLSI hardware) [10].

3. Evaluation metrics

- **Encryption Time:** The time taken by an encryption algorithm to convert plaintext data to ciphertext refers to encryption time. It is an indicator of the efficiency of the algorithm. In the following analysis the encryption time is measured in milliseconds and is considered a factor determining the speed of encryption in wireless networks.

- **Decryption Time:** The time taken by an encryption algorithm to convert ciphertext data to plaintext data refers to decryption time. Lesser the decryption speed, more is the efficiency of the algorithm. In the following analysis decryption time is measured in milliseconds and it also is used to determine speed of the wireless network.

- **Throughput:** The throughput of a cryptosystem is the megabytes of plaintext encrypted per millisecond by the algorithm. A greater throughput is indicative of a more efficient system. The unit of measurement is MBps.

4. Experimental Design

The analysis has been performed using the encryption algorithms, viz. AES, Blowfish and Twofish implemented in python 3.6.9 on a Laptop having 3.8GHz Intel i5-9300H processor with 8GB RAM on Ubuntu 18.04, Linux kernel 5.3.0-53. The algorithms are tested on a text file of size 1.1 MB.

5. Results and Discussion

The analysed data are presented in Table 1, 2 & 3 and Figure 1 & 2, and discussed accordingly.

Table 1: Comparison of Encryption time (in ms) of the Algorithms

Algorithm	Encryption time (in ms)
AES	8.9
Twofish	3.1
Blowfish	4.2

Table 2: Comparison of Decryption time(in ms) of the Algorithms

Algorithm	Decryption time (in ms)
AES	7.4
Twofish	4.1
Blowfish	4.9

Table 3: Comparison of Throughput (in MBps) of the Algorithms

Algorithm	Throughput (in MBps)
AES	1236
Twofish	3548
Blowfish	2619

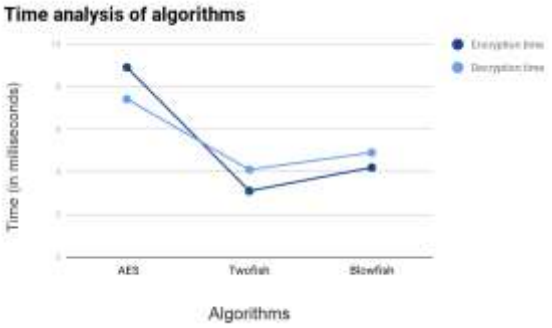

Fig. 1: Time analysis of the algorithms: AES, Twofish and Blowfish

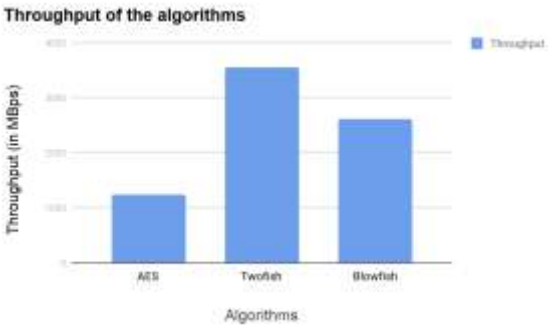

Fig. 2: Comparison between the throughput of the algorithms: AES, Twofish and Blowfish

The algorithms, viz. AES, Blowfish and Twofish have been implemented and the encryption time and decryption time have been noted, and the throughput calculated separately for each algorithm. The result indicates that Twofish has the best performance followed by Blowfish and AES owing to its least encryption and decryption time (Table 1 & 2 and Fig.1) and the maximum throughput (Table 3 and Fig.2).

The superiority of Blowfish over AES in prevention of guessing attacks was reported by Wahid *et al*. (2018) [11], and in another experiment, the superiority of Twofish over Blowfish was reported earlier by Rane (2016) [12]. These findings are in agreement with the present result.

6. Conclusion

Twofish has a clear advantage over AES and Blowfish in terms of the evaluation metrics studied, *viz*., encryption time, decryption time and throughput. Hence, Twofish can be implemented alongside HMAC in the security of all networking protocols owing to its low encryption and decryption time, and high throughput.

7. References

1. Bono, S.C., Green, M., Stubblefield, A., Juels, A., Rubin, A.D., Szydlo, M. (2005) Security analysis of a cryptographically-enabled RFID device. In: SSYM'05: Proceedings of the 14th Conference on USENIX Security Symposium, August 1-5, 2005, Baltimore, USA.

2. Bellare, M., Canetti, R. and Krawczyk, H. (1996) Message Authentication using Hash functions-The HMAC Construction. RSA Laboratories' CryptoBytes, Vol 2, No. 1.

3. Stallings, W. (2017) Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson India Education Services Pvt.Ltd., Noida, Uttar Pradesh, pp. 89, 172-190.

4. Polimon, J., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A. (2008) Automated design of a lightweight block cipher with genetic programming. Int. J. Know-Based Intell Eng. Syst.,12(1):3-14.

5. NIST (2001) Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST).

6. Nechvatal, J.,Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. and Roback, E. (2001) Report on the Development of the Advanced Encryption Standard (AES). Journal of Research of the National Institute of Standards and Technology, 106(3):511-577.

7. Nyberg, K. (1991) Perfect nonlinear S-boxes. In: Davies, D. W. (eds) Advances in Cryptology — EUROCRYPT. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Germany.

8. NIST (2001) Federal Information Processing Standards Publication 197, Announcing the Advanced Encryption Standard (AES).

9. Schneier, B. (1993) Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop Proceedings. Springer-Verlag, pp. 191–204.

10. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N. (1998) Twofish: A 128-bit block cipher, pp.1-68.

11. Wahid, M.N.A., Ali, A., Esparham, B. and Marwan, M. (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. Journal of Computer Science Applications and Information Technology, 3(2); 1-7.

12. Rane, D. D. (2016) Superiority of Twofish over Blowfish. International Journal of Scientific Research and Management, 4(11): 4744-4746.

Biography

Archisman Ghosh is currently pursuing B. Tech. in Computer Science & Engineering (Batch 2019-23) at National Institute of Technology, Durgapur, an institute of national importance in India. His area of interest includes algorithms, cryptography, network security, and machine learning.