Analyze the Avalanche effect and its strength in Cryptographic Algorithms

Amruta J.Thakur
Department of Computer Science,
Science College,
Nagpur-440010

Prof. R. N. Jugele
Department of Computer Science,
Science College,
Nagpur-440010

Abstract:
Developments in computers and technologies have created an intense need for secure and trustworthy cryptography systems. Highly secure schemes are always desirable for real-world applications. Cryptography requires a secure technique to ensure that the enemy is prevented while securing legitimate users who have access to the data. The avalanche effect is one of the most preferred approaches for determining an algorithm's security in cryptography. This paper aims to analyze the Avalanche Effect and its Strength in two most commonly used symmetric encryption algorithms AES and Blowfish. Avalanche effect is considered as one of the desirable property of any encryption algorithm, a slight change in either the key or the plain-text should result in a significant change in the cipher-text helps to increase the strength of any algorithm. The paper concluded by analyzing that AES exhibits a strong avalanche effect.

Keywords: Avalanche effect, cryptography, AES, Blowfish, cyber attacks

1) Introduction:

Cryptography is the practice and study of hiding information. For secure communication over public network data can be protected by the method of encryption. Encryption converts that data using an encryption algorithm using the key in scrambled form. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data [2]. During the encryption process, scrambled data can be understood only by the authorized parties. The main goal of data encryption is to preserve the information from cyber-attacks [7]. AES and Blowfish are falls into this category, meaning it uses the same key to encrypt and decrypt data. The strength of these algorithms is analyzed using the three features the use of keys, the nature of algorithms and timing attacks.

2) The Strength of AES and Blowfish:

- The use of keys
- The nature of algorithms
- Timing Attacks

AES (Advanced Encryption Standard): AES also known as Rijndael, is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text [2]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an Add Round Key stage. Timing attacks assumes that an attacker knows how long a particular encryption operation takes.

Blowfish: Blowfish is a keyed symmetric block cipher designed in 1993 by Bruce Schneider. Schneider designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. 18 sub-keys are derived from a single initial key. It requires total 521 iterations to generate all required sub keys. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. Its structure which uses fixed S-boxes. Blowfish performs well for applications in which keys does not change often. The small 64-bit block size makes the algorithm vulnerable to birthday attacks, a class of brute-force attacks.

Strength of AES	Strength of Blowfish
• AES is widely regarded as highly secure. It has been adopted by the U.S. government and is used worldwide to protect sensitive data.	• Blowfish was designed to be highly secure, and it has withstood extensive cryptanalysis.
• AES supports key lengths of 128, 192, and 256 bits. The longer the key, the stronger the encryption.	• Blowfish supports variable key lengths from 32 bits up to 448 bits. Longer key lengths generally provide stronger security.
• AES is computationally efficient, making it suitable for use in a wide range of applications, including embedded systems and high-performance computing environments.	• Blowfish is relatively fast and efficient, making it suitable for many applications. However, compared to AES, it may not be as optimized for performance in certain scenarios.
• No practical vulnerabilities have been discovered in the AES algorithm. The security of AES depends on the strength of the key and the implementation of the algorithm.	• While Blowfish has been widely used and analyzed for many years without significant vulnerabilities being found, it is considered less secure than AES, especially as time goes on and cryptanalysis techniques improve.

Table1: Strength of AES and Blowfish encryption algorithms [8]

3) Avalanche Effect: The avalanche effect in cryptography refers to the property where a small change in input (plaintext or key) results in a significantly different output (cipher text or hash). It's a crucial aspect of cryptographic algorithms, ensuring that even minor alterations to the input data propagate throughout the encryption or hashing process, making it difficult for attackers to discern any patterns or extract meaningful information from the output without knowledge of the key[1]. Here's a simplified diagram illustrating the avalanche effect in a cryptographic algorithm.

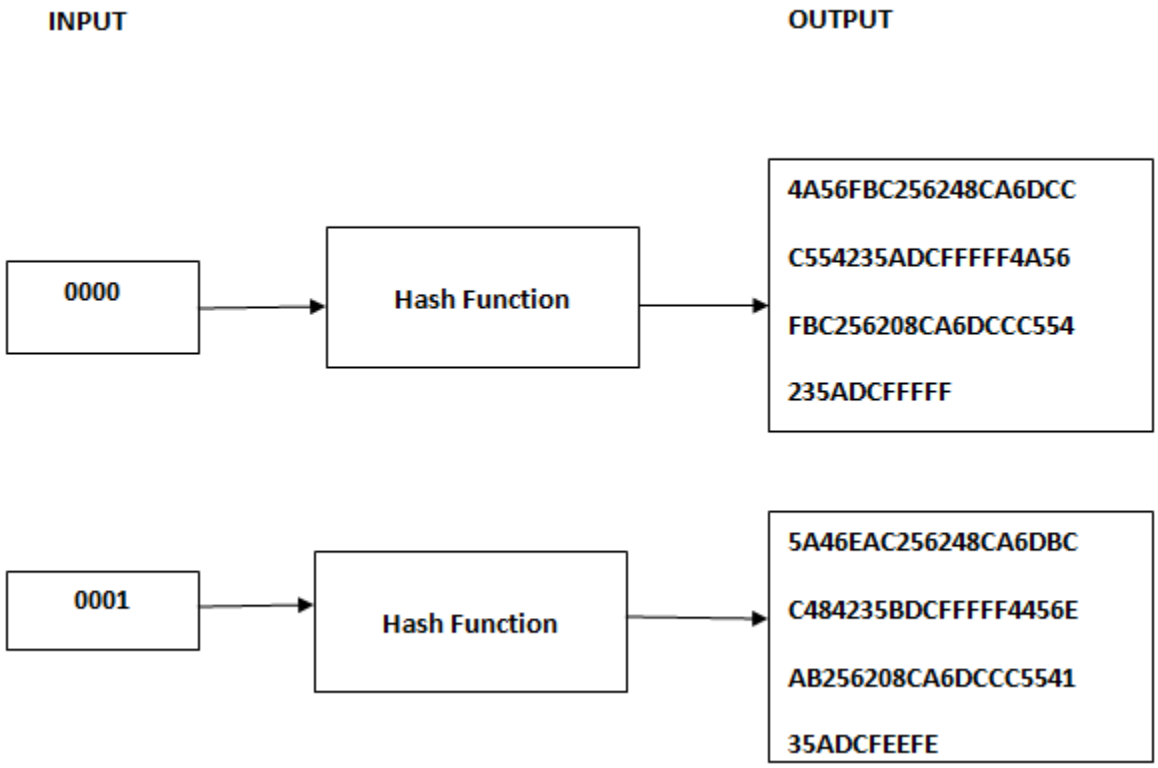

Fig 1: Avalanche Effect

In case of algorithm that uses hash value, even a small alteration in an input string should drastically change the hash value. In other words, flipping single bit in input string should at least flip half of the bits in the hash value [6]. A good encryption algorithm should always satisfy the following relation:

Avalanche effect > 50%

Basic structure of both algorithms and how they exhibit the avalanche effect:

AES (Advanced Encryption Standard): Plaintext --[Key XOR]--> Round 0 --[SubBytes]--> Round 1 --[ShiftRows]--> Round 2 --[MixColumns]--> Round 3 --[AddRoundKey]--> ... -->

Round 9 --[SubBytes]--> Round 10 --[ShiftRows]--> Round 11 --[MixColumns]--> Round 12 --[AddRoundKey]--> Ciphertext[9]

Each round of AES involves several operations such as SubBytes (byte substitution), ShiftRows (row shifting), MixColumns (column mixing), and AddRoundKey (round key addition)[2]. The output of each round serves as the input to the next round. Even a small change in the plaintext or the key results in a drastically different cipher text due to the avalanche effect[3].

Blowfish: Plaintext --[Key Expansion]--> Round 1 --[Substitution]--> Round 2 --[Permutation]--> Round 3 --[Key Mixing]--> ... --> Round 16 --[Substitution]--> Round 17 --[Permutation]--> Round 18 --[Key Mixing]--> Cipher text[5]

Blowfish operates in a Feistel network structure, where each round consists of substitution, permutation, and key mixing operations. The key expansion phase generates round keys used in each round. Similar to AES, even a small change in the plaintext or the key results in a significant change in the cipher text due to the avalanche effect[4].Here, we'll compare the avalanche effect of the AES and Blowfish algorithms. We'll change a single bit in the plaintext and observe how the cipher text changes. Using javax.crypto package for AES and Blowfish algorithms.

Key Generation: We generate 128-bit keys for both AES and Blowfish algorithms.

Encryption: The encrypt method encrypts the plaintext using the specified algorithm.

Plaintext Modification: We modify the plaintext by flipping one bit.

Avalanche Effect Calculation: The Avalanche Effect method calculates the percentage of bit changes between the original and modified cipher texts.

Output shows the avalanche effect in percentage for both AES and Blowfish, helping to compare their sensitivity to small changes in the plaintext.

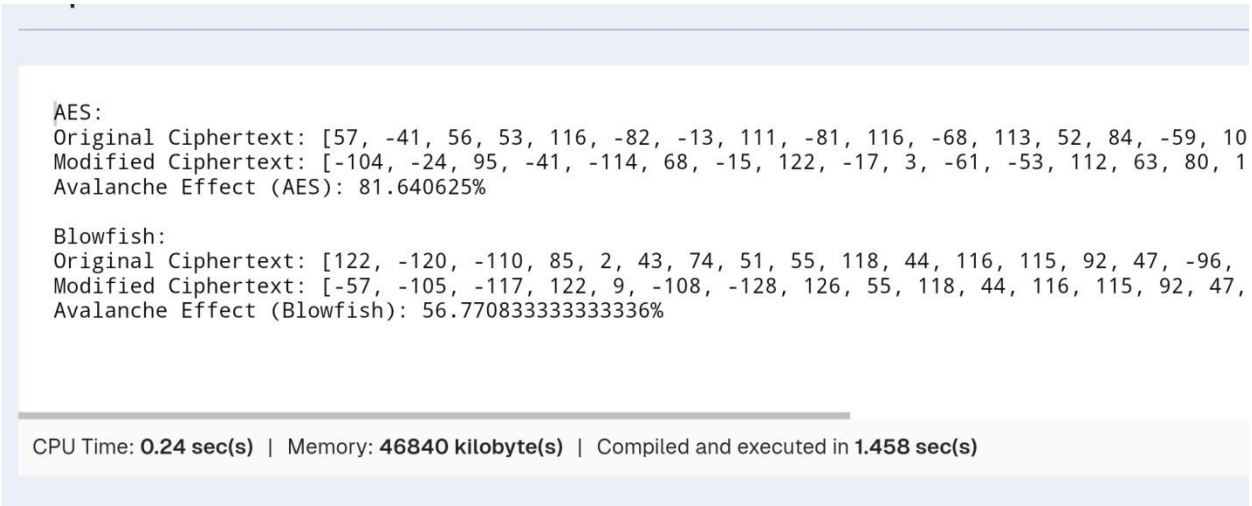

Fig 2: Output of Avalanche effect calculation

The proportion of bits that change in the output when a single bit is changed in the input. When a single bit in the input of AES is changed, approximately 81.640625% of the output bits change. This indicates a high avalanche effect, suggesting that AES exhibits strong diffusion properties, where changes in the input are well-dispersed throughout the output.

Similarly, for Blowfish, when a single bit in the input is changed, approximately 56.7708333% of the output bits change. This indicates a lower avalanche effect compared to AES. While Blowfish still exhibits diffusion, it's not as strong as AES based on this metric.

4) Prevention from Cyber Attacks: Both AES (Advanced Encryption Standard) and Blowfish benefit from the strength in avalanche effect, which contributes to their resilience against various types of cyber attacks[11]. However, the effectiveness of this property in preventing specific attacks may vary between the two algorithms.

AES, being a more recent encryption standard adopted by organizations and governments worldwide, has undergone extensive analysis and scrutiny. Its design includes features that enhance security against known cryptographic attacks. The Rijndael algorithm, upon which AES is based, exhibits a strong avalanche effect, making it highly resistant to differential and linear cryptanalysis, among other attacks. AES's design features and extensive scrutiny contribute to its robustness against a wide range of cyber attacks such as Brute Force Attacks, Differential Cryptanalysis and Linear Cryptanalysis.

Blowfish, while also benefiting from the strength in avalanche effect, is an older encryption algorithm designed by Bruce Schneier. It has not undergone as much formal scrutiny as AES and is generally considered less secure for new applications requiring high levels of security. While Blowfish's avalanche effect helps protect against certain cryptographic attacks, it may not provide the same level of security assurance as AES due to factors such as key size limitations and potential vulnerabilities discovered over time.

Both AES and Blowfish benefit from the strength in avalanche effect, which contributes to their resilience against cryptographic attacks[1]. However, AES, with its advanced design features and extensive scrutiny, may offer stronger protection against a wider range of cyber attacks compared to Blowfish.

5) Conclusion: The avalanche effect ensures that encrypted data is highly sensitive to changes, making it difficult for attackers to derive any meaningful information from the cipher text without knowledge of the correct key. Cryptographers rigorously analyze and test symmetric algorithms to verify their avalanche properties, ensuring their effectiveness in real-world security applications. Both the AES and Blowfish algorithms exhibits strong diffusion. However the comparison between the Avalanche percentage emphasizing AES algorithm exhibits a strong avalanche effect.

References:

[1] Kamsiah Mohamed , Mohd Nazran Mohammed Pauzi , Fakariah Hani Hj Mohd Ali, ANALYSE ON AVALANCHE EFFECT IN CRYPTOGRAPHY ALGORITHM, ICONSPADU 2021 International Conference on Sustainable Practices, Development and Urbanisation.

[2] Youssouf Mahamat koukou, Siti Hajar Othman, Maheyzah MD Siraj. Herve Nkiama, Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithms, IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN (e): 2250-3021, ISSN (p): 2278-8719.

[3] Drashti O. Vadaviya , Purvi H. Tandel ,Study of Avalanche Effect in AES, NCRAES

[4] Security analysis of blowfish algorithm, Ashwaq Mahmood Alabaichi, Conference: Informatics and Applications (ICIA)

[5] Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data, Abidemi Emmanuel Adeniyi

[6] Avalanche Effect in Cryptography - GeeksforGeeks

[7] Jagpreet Kaur; K.R. Ram Kumar, Analysis of Avalanche effect in Cryptographic Algorithms, Publisher: IEEE, 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2022, pp. 1-4, doi: 10.1109/ICRITO56286.2022.9965127.

[8]Strengths and Weaknesses of AES | Download Table (researchgate.net)

[9] AES Timing Attack - Schneier on Security

[10] Rohit Verma , Aman Kumar Sharm,"Cryptography: Avalanche effect of AES and RSA", International Journal of Scientific and Research Publications, Volume 10, Issue 4, April 2020 119 ISSN 2250-315

[11]DARSHANA UPADHYAY 1 , NUPUR GAIKWAD1 , MARZIA ZAMAN 2 , AND SRINIVAS SAMPALLI 1 , (Member, IEEE)"Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based "Digital Object Identifier 10.1109/ACCESS.2022.3215778