A Novel Recommendation To AES Limitation

Falguni Patel, Mohammed Farik

Abstract: Among all available conventional encryption algorithms, the AES (Advanced Encryption Standard) is the most secured and highly used algorithm. AES algorithm is widely used by variety of applications like Archive and Compression tools, File Encryption, Encryption File System, Disk / Partition Encryption, Networking, Signal Protocol, among others. This paper highlights the Brute Force attack and Cryptanalysis attack on AES Algorithm. This paper also discusses about a novel recommendation of a combination model of AES Algorithm and Random-X Cipher.

Index Terms: AES, Random-X Cipher, Cryptanalysis Attack, Brute-Force Attack

1 Introduction To Symmetric Algorithm

The AES is the most popular, fast and secure Symmetric Algorithm. The ingredients of Symmetric algorithm are – Plain Text, Encryption Algorithm (AES), Secret Key, Cipher Text and Decryption Algorithm [1]. The Secret Key plays the major role in this Encryption Algorithm [2]. As shown in Fig. 1, the ciphertext Y generated by AES Algorithm relies on the Secret Key K-shared by sender and receiver. Since only one Secret Key is shared by sender and receiver for encryption and decryption, it is also called Secret key or Single Key Encryption.

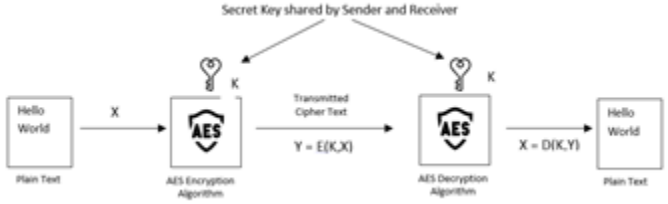

Fig. 1 *Symmetric Algorithm (AES) Simplified Model [1]*

2 Possible Attacks on AES Algorithm

2.1 The Brute Force Attack

The Brute Force approach tries all possible combinations of Secret keys to decrypt the Cipher Text [1]. Length of this secret key decides the strength of the Encryption algorithm. A 4-bit key can have 16 possible combinations. Similarly, a 128-bit key can have 3.4 x 10^{38} possible combinations. Longer secret keys can have more combinations than shorter secret keys. Hence, Brut Force attack will require longer time to try all possible combinations. As discussed by Arora in EE Times, it is nearly impossible to crack the AES-128 algorithm with Brute Force Attack with current available resources [3], [4]. However, the attacks are possible with these three possibilities. Firstly, AES algorithm will no longer be secured when the Quantum technology become more available and powerful.

- *Falguni Patel is a Project Manager – Enterprise Resource Planning (ERP) at Motibhai Group of Companies Ltd – Fiji Islands and a student of Masters in Information Technology at UniFiji, Saweni Campus. Ph: + 679 6668941. Email: falguni_divyesh@yahoo.co.in or falguni.divyesh@gmail.com.*
- *Mohammed Farik (Member, IEEE) is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

Secondly, the Brute force attack can become more powerful by filtering only possible combinations which will certainly reduce the number of combinations resulting reduced time to try all combinations. Thirdly, there is a possibility of achieving success after trying less than 50% of combinations only.

2.2 Cryptanalysis Attack

The Cryptanalysis can have various types of attacks like Ciphertext only, Known plaintext, Chosen plaintext, Chosen Ciphertext and Chosen text attacks [1]. Since larger secret keys will have large combinations of possible keys, Brute Force attack is infeasible with current available resources. The Cryptanalysis Attacks have high success rate when an attacker has a known plaintext or manages to get the source system to insert into the message selected by analyst [1]

3 Novel Recommendation To Improve AES Functionality

The additional encryption function that uses Random-X cipher can be used between the plain text and AES Algorithm. As mentioned by Falguni and Farik, the Random-X cipher substitutes the each character of plaintext with three (or more) random characters string. Since the encrypted result string of the same input string varies every time the string is encrypted, the cryptanalysis of Random-X cipher is difficult [5].

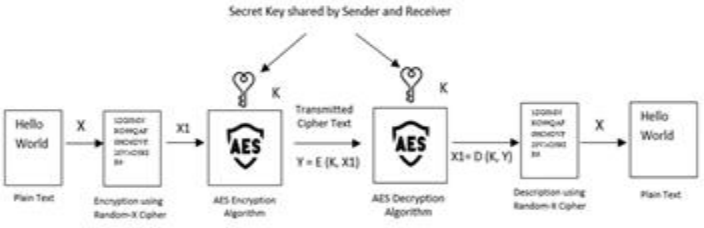

Fig. 2 *Simplified block diagram of AES Encryption using Random-X Cipher*

As shown in Fig. 2, instead of passing the plain text X directly to AES Algorithm, the Plaintext X is now passed to an additional Encryption function which uses the Random-X Cipher. The output of this Encryption - an encrypted text X1 is passed as an input text to AES Encryption Algorithm. The AES algorithm converts the Encrypted Text X1 into Cipher Text Y. The Decryption process is the reversal of Encryption process. The Cipher Text Y is first passed through the AES Decryption Algorithm and outputs Encrypted Text X1. This Encrypted text X1 is then passed to the Description of Random – X Cipher function and the final result is an original Plain Text. The addition of a Random-X cipher based Encryption Algorithm protects the AES algorithms against Brute Force Attack and Cryptanalysis attack.

3.1 The Protection against Brute Force Attack

As discussed in this recommended solution, the input to the AES Algorithm is an Encrypted text using Random-X Cipher. If the AES Algorithm is compromised and an attacker has managed to decrypt the AES Algorithm, the output of this attack is an Encrypted Text X1. The attacker is expecting the meaningful text as an output. As shown in Fig. 2, if an attacker has managed to crack the AES Algorithm using Brute Force Attack, the output is '1ZG0MNKO99QAF0HO6DVF20VXO3KIR9'. This is meaningless to an attacker. It is nearly impossible for an attacker to retrieve 'HelloWorld' from output text '1ZG0MNKO99QAF0HO6DVF20VXO3KIR9'.

3.2 The Protection against Cryptanalysis Attack

As discussed in Section 2.2 of this paper, Cryptanalysis attack on AES has high success rate when the attack is based on known plaintext and chosen plaintext. The recommended solution protects the system against these attacks because the input to the AES is an Encrypted Text X1 resulted from the Random-X cipher. As shown in Fig. 2, the input to the AES Algorithm is '1ZG0MNKO99QAF0HO6DVF20VXO3KIR9' instead of 'HelloWorld'. Hence, the result of this attack will be '1ZG0MNKO99QAF0HO6DVF20VXO3KIR9' instead of 'HelloWorld'. Moreover, the Random-X based Encryption will always produce a different output string for the same word – 'HelloWorld' [5] due to its characteristics of randomly assigning substitution value. This indicates that the Encrypted Text X1 (input) to AES algorithm and Cipher text Y (output) from AES algorithm for the same word 'HelloWorld' will not be identical for each test. This characteristic makes the Cryptanalysis of Random-X Cipher merely impossible. Hence, the messages protected with the combination of Random-X cipher an AES algorithm are impossible to crack with Cryptanalysis attack.

4 Conclusion

The combination of AES Algorithm and Random-X based Algorithm model recommended in this paper, protects the message or communication with great efficiency. This combination will help overcome the limitations of AES Algorithm against Brute Force Attack and Cryptanalysis attack.

References

[1] W. Stallings, Network Security Essentials: Applications and Standards, Fourth Edition ed., NJ: Pearson Education, Inc., publishing as, 2011, pp. 27-60.

[2] Microsoft, "Data Confidentiality," 2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff650720.aspx. [Accessed 08 06 2017].

[3] M. Arora, "How Secure is AES against Brute Force Attacks - EE Times," 2012. [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1279619. [Accessed 20 04 2017].

[4] Reddit, "Time and Energy required to brute-force a AES-256 encryption key," 2017. [Online]. Available: https://www.reddit.com/r/theydidthemath/comments/1x50xl/time_and_energy_required_to_bruteforce_a_aes256/. [Accessed 10 06 2017].

[5] F. Patel and M. Farik, "A New Substitution Cipher - Random-X," International Journal of Scientific and Technology Research (IJSTR), vol. 5, no. 10, pp. 125-128, 2016.