DALHOUSIE UNIVERSITY

Faculty of Computer Science

CSCI 6708 – Advanced Topics in Network Security

Name: Arka Ghosh
Banner ID: B00911033
Assignment: 05

Overview of Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetrical block cipher algorithm that takes inputs in block of 128 bits and transforms these particular blocks using keys of 128, 192 and 256 bits [1]. In 1997, The National Institute of Standards and Technology (NIST) started to develop AES when it identified the need for a replacement to the Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks [2]. AES is widely used today because it is substantially more powerful than DES and triple DES.

Features of AES

- AES works on a substitution-permutation network structure rather than a Feistel Cipher Structure [3].
- The AES encryption process works with byte data instead of bit data. As a result, during the encryption process, it treats the 128-bit block size as 16 bytes [1].
- During the initial state, it just takes a single key which is later expanded on multiple keys in each individual rounds [1].
- The number of the rounds is determined by the key size that is being used. There are 10 rounds for a 128-bit key, 12 rounds for a 192-bit key and 14 rounds for a 256-bit key [3].

AES Algorithm Description

Each round in AES consists of the following steps (Appendix A) to produce the cipher text:

- **Add Round Key:** The block data stored in the state array is sent via an XOR function with the initial key created (K0), which is used as an input in the following phase (appendix B).
- **Sub-bytes:** Each byte is substituted by another byte using a looking up table called S-box in this step (appendix B). The result of this step in a (4 x 4) matrix like the previous step.
- **Shift Rows:** Each row is shifted a particular number of times in this step (appendix B). It skips the first row, and starts shifting the elements one position left in the second row, two positions left in the third row and three positions left in the fourth row.
- **Mix Columns:** This is a matrix multiplication step which multiples each column with a specified matrix, resulting in a change of each byte's location in the column (appendix B).
- **Add Round Key:** The preceding stage's resulting output is XORed with the round key (Appendix B). The resultant state array becomes the cipher text for the specified block if this is the final round; otherwise, it becomes the new state array input for the next round.

The decryption process is the reverse of the encryption process which consists of four steps i.e. Add Round Key, Inverse Mix Columns, Shift Rows and Inverse Sub Byte in each round.

Advantages and Drawbacks of AES

AES uses higher length of key sizes which provides stronger encryption by being resistant to brute force attacks. It is proved very resistant to differential, linear, interpolation and square attacks, in comparison to 3DES, which is sensitive to differential and linear cryptanalysis [4]. Additionally, this algorithm allows SSL/TLS encryption protocols to always surf with the highest security and privacy since it uses both symmetric and asymmetric encryption [1]. Although this robust security algorithm can be implemented in both hardware and software, AES in counter mode is comparatively difficult to implement in software considering its security [5].

References

[1] "What Is AES Encryption and How Does It Work?", *Simplilearn*, 2022. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. [Accessed: 24- Mar- 2022].

[2] C. Bernstein and M. Cobb, "What is the Advanced Encryption Standard (AES)? Definition from SearchSecurity", *SearchSecurity*, 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard. [Accessed: 24- Mar- 2022].

[3] A. Zohair Mustafeez, "What is the AES algorithm?", *Educative: Interactive Courses for Software Developers*, 2022. [Online]. Available: https://www.educative.io/edpresso/what-is-the-aes-algorithm. [Accessed: 24- Mar- 2022].

[4] N. Aleisa, "A Comparison of the 3DES and AES Encryption Standards", *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 241-246, 2015. Available: 10.14257/ijsia.2015.9.7.21.

[5] "Advantages of AES | disadvantages of AES", *Rfwireless-world.com*, 2022. [Online]. Available: https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html. [Accessed: 24- Mar- 2022].

Appendix

Appendix A

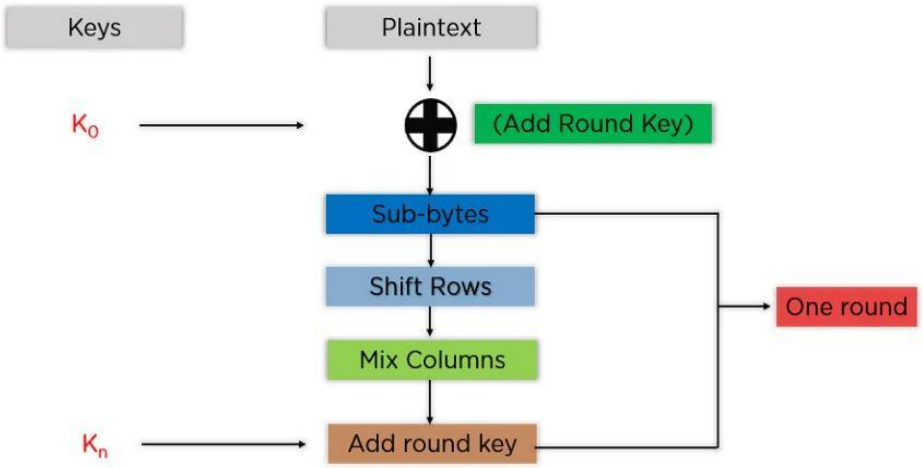

Figure 1: Steps in Each Round of AES Algorithm [1]

Appendix B

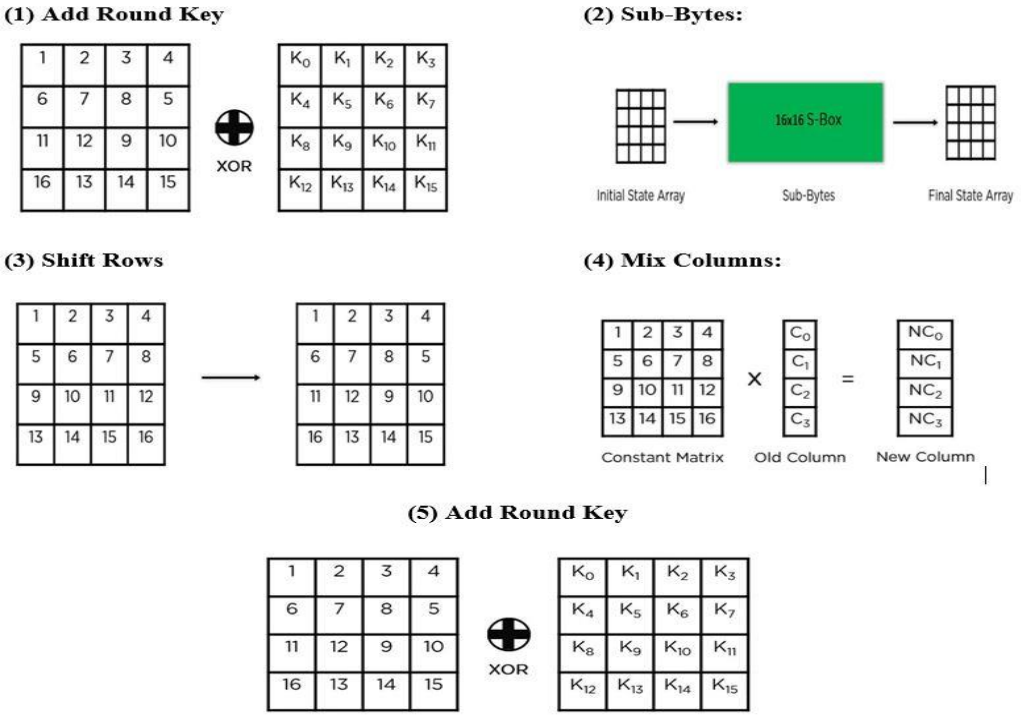

Figure 2: Demonstration of Each Step in AES Algorithm [1]