ASSIGNMENT – 4

CSCI-6708 Advanced Network Security

Sumit Singh

B00882103

Sm435410@dal.ca

Exercise -1

Advantaged Encryption Standard (AES)

The Advantaged Encryption Standard (AES) is a fast and secure form of encryption that ensures that our data is safe. It is been around since 2001 and still considered as one of the best encryption processes. Top chat application like WhatsApp and Signal also uses AES for end to end encryption, programs like VeraCrypt and WinZip are based on AES. AES has become the best available encryption since it was introduced.

As DES was introduced 40 years ago by Government of USA and by 1990's people were getting better at cracking code. The encryption had to become sophisticated so that massages could be kept secret and safe. After US set a program to get a better encryption, in 2001 the National Institute of standard and technology (NIST) announced that it had finally selected an encryption algorithm. Encryption always came with a tradeoff. You can either go with simple algorithm or complex like AES, but it will mostly cost the processing time for encryption and decryption as we chose complex encryption. Finally, NIST chose the Rijndael block cypher for its all-around capabilities, including its performance on both hardware and software, ease of implementation, and level of security.

Following are the steps data go through during AES Encryption, firstly data is divided into blocks depending on the key length. If it is 128 bits key then data is divided into 4 * 4 column of 16 bits (16 * 8 = 128). Then comes key expansion which we use in the further steps to come up with keys for each round of encryption process. Then add key and substitute bites which leads to non-liner arrangements and hence causes confusion. Then we shift rows and mix columns to make it more unrelated to plain text. Finally add round key again. This process is repeated multiple times based on key length.

Why these steps:

Key expansion is a critical step because it generates the keys which are important for next rounds, else we will be using same key for each step and it would be easy to crack.

Byte substitution is an important step because it changes the data points based on the predefined table. This leads to the confusion as data is altered in nonlinear way.

Shift row is used to perform diffusion which transpose the data to add complications.

We need a greater number of rounds to avoid brute-force attach like shortcut attack and also adding more rounds ensures stronger security. The 10, 12 and 14 rounds of ARE standardized because that is enough to make sure that we are secure from attack. Adding more rounds makes it even secure but we might have to compromise on the speed.

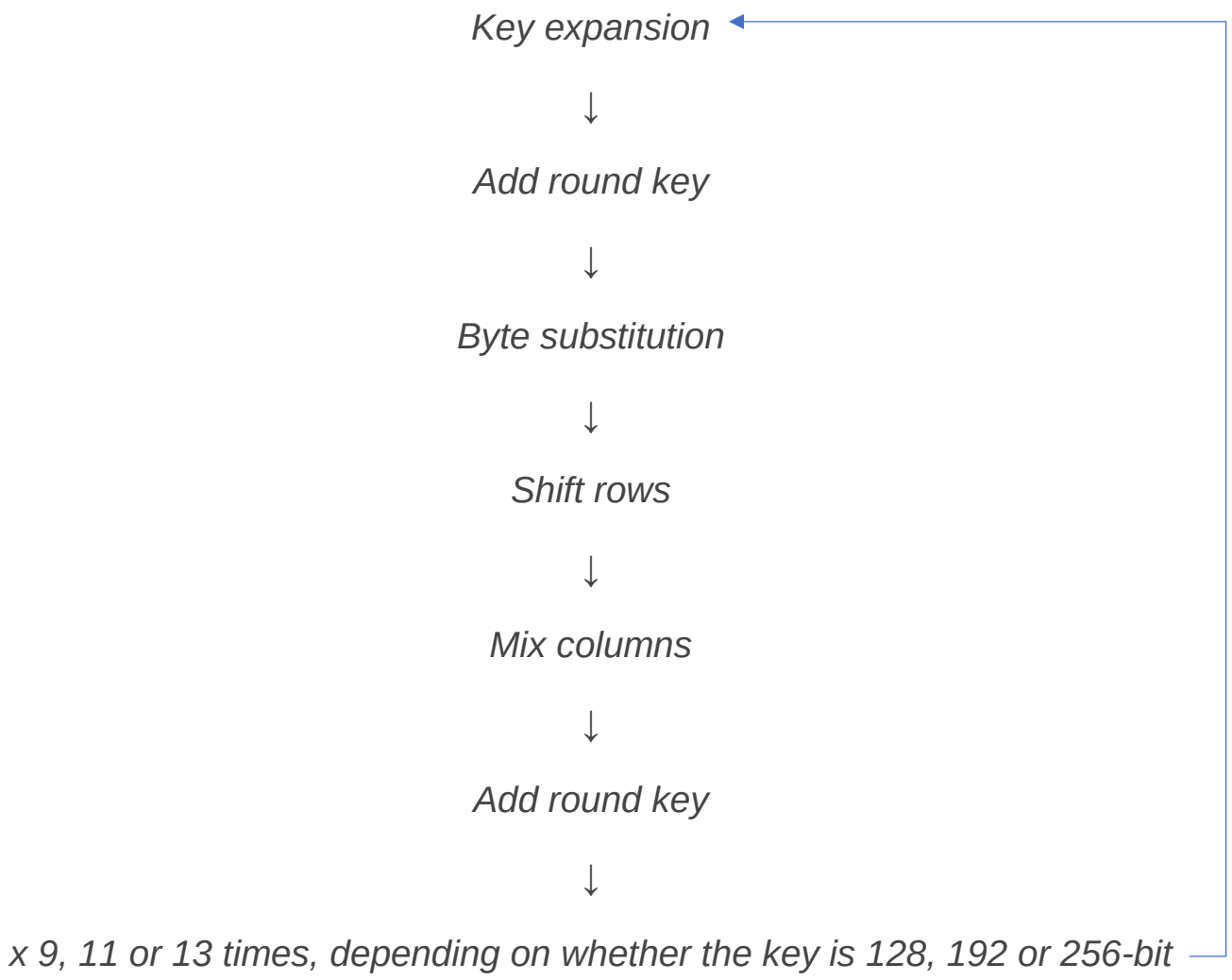
Key lengths of AES define the number of rounds this data processing would go through. 128, 192- and 256-bit AES are standard key length but 192 and 259 bits provide greater security margin when compared to 128.

Even AES has some security issues. There are some research that claim theoretical breaks and side attach attacks. Some of the knows attacks are knowledge key distribution attack which was a success on 8 round version, so there is not much to worry about as we are mostly using 10 round

version. Related key attack is the other theoretical attack, this is mostly possible only on protocols those are not implemented properly.

Regardless of current theoretical attacks or potential side-channel attacks, AES remains secure. It is an excellent standard for securing our electronic communication and can be used in a variety of situations where sensitive information must be safeguarded. Based on current technology and attack techniques, you should be able to use it with confidence for the foreseeable future.

Brief process of encryption:



Exercise -1

Advantaged Encryption Standard (AES)

References:

[1]"What is AES encryption (with examples) and how does it work?", *Comparitech*, 2022. [Online]. Available: https://www.comparitech.com/blog/information-security/what-is-aes-encryption/#128_vs_192_vs_256-bit_AES. [Accessed: 05- Apr- 2022].

[2]"What is the Advanced Encryption Standard (AES)? Definition from SearchSecurity", *SearchSecurity*, 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard. [Accessed: 05- Apr- 2022].

[3]"Advanced Encryption Standard - Wikipedia", *En.wikipedia.org*, 2022. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 05- Apr- 2022].

[4]"Advanced Encryption Standard", *Tutorialspoint.com*, 2022. [Online]. Available: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm. [Accessed: 05- Apr- 2022].