DALHOUSIE UNIVERSITY

Network Security (CSCI-6708)

Assignment - 6

Shivam Gupta
B00810723

Advance Encryption Standards (AES)

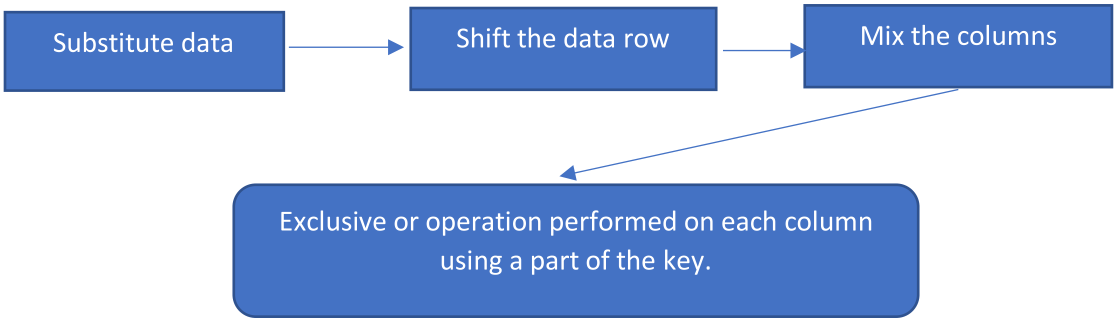
- Symmetric block cipher to protect confidential and classified information.
- Used in hardware and software to encrypt sensitive data and information.
- Developed in 1997.
- Successor algorithm of Data Encryption Standards (DES).
- Easy to implement and offer great defence against various attacks

Features of AES:

- Very secure and easy to implement. Safe against brute force attacks.
- Cost efficient and globally available.
- Computational and memory efficiency.
- Simplicity: easy to use.
- Fast and reliable.

Algorithm Used:

- 3 block ciphers: AES-128, AES-192, AES-256
- They have many rounds according to the type of block cipher and each round has various processing steps including substitution, transposition, and mixing of input plaintext and transform into final cipher text [1].
- Process:



Substitute data

Shift the data row

Mix the columns

Exclusive or operation performed on each column using a part of the key.

AES-128	AES-192	AES-256
• AES-128 uses 128 bits key to encrypt/decrypt messages. • There are 10 rounds	• AES-192 uses 192 bits key to encrypt or decrypt. • There are 12 rounds.	• AES-256 used 256 bits key to encrypt/decrypt. • There are 14 rounds.

Advantages	Drawbacks
1. Exponentially faster than other algorithms. 2. Mathematically efficient and can even work well with quantum computers.	1. Encryption keys needs to be protected. 2. Doesn’t block social engineering and phishing attacks. 3. Low security for side channel attack.

References:

[1] Advanced Encryption Standard (AES), Margaret Rouse, https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard,