NIST Standard that specifies AES: https://csrc.nist.gov/pubs/fips/197/final

AES Operations

XOR - Exclusive OR Operation

Confusion - relationship between the key and the cipher text, desirable to have this be complicated so that the ciper text and the key does not provide information about the plaintext

Diffusion - the statistical patterns in the cipher text, desirable to have a small change in the plain text lead to a large change in the cipher text

Choose mathematical operations that are difficult to reverse

AES is a block cipher, keys can be 128, 192, or 256 bits in length

The plaintext blocks will always be 128 bits in length
The cipher text output will always be 128 bits in length

16 bytes = 128 bits

State Array: Put 16 bytes in a 4x4 matrix, sometimes called the state of the algorithm

Need a key that is the same size grid of bytes

Adding the key to the state = XOR key with plain text to form a new state of the grid

How AES creates confusion:

Key Expansion

- AES specifies a key expansion algorithm to create N 16 byte keys from the original key
- Each bit in an expanded key depends on bits in the previous key
- Combine bit values from previous keys, swap bits, shift bytes around
- Applying rounds of transformation adds complexity to the process
- 128 bit key = 11 rounds, 192 bit key = 13 round, 256 bit key = 15 rounds

Substitution Ciphers

- AES using substitution bytes
- Each byte in the state is replaced with its substitution
- Substitution function uses complex algebra

Each round consists of an XOR operation with a round key, then a byte substitution operation

Combining these two operations provides more confusion that than either technique does alone

How AES creates diffusion:

- Shift rows then mix columns
- Shift rows
    - The rows are permuted by circular shifts left
        - The leftmost byte(s) are moved to the right end of the row
    - The first row is unchanged
    - The second show is shifted left by 1 byte
    - The third row is shifted left by 2 bytes
    - The fourth row is shifted left by 3 bytes
- The mix columns step combines the values in the other bytes to get new values
    - Multiplication and addition operations performed using the other bytes in the column
    - These multiplication and addition operations use **finite field arithmetic operations** that restrict the values to {0,...,255} that will fit in a byte (8 bits)

Basic steps in each round:

XOR round key
Substitute bytes
Shift rows
Mix columns
XOR the round key again