**Class Notes AES**

**Monday September 20th, 2021**

**Rijndael Cipher Algorithm:**

The winner of the AES selection. Uses 128-bit message size with 128/192/256 bit keys

10 Rounds for 128 bit, 12 for 192, 14 for 256.

A block cipher mechanism that takes in a cipher key, along with the plaintext, and encrypts it to provide us a cipher text.

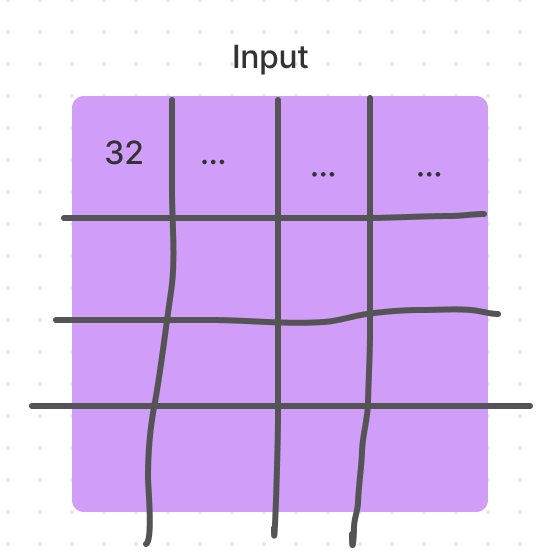
A different cipher key is generated for each round.

Message space = 2^128

Key Space = 2^128 or 2^192 or 2^256

Cipher Text = 2^128

The Input 16 blocks of 8 bits = 128 bits



**The Encryption Process**

**Add Round key**

**1-Sub Bytes (Substitution Table)**

The first number is the row, the second number is the column

Example: 19 -> 1 is the row, and 9 is the column. The subbed byte is the intersection of the two

**2-ShiftRows**

1st row doesn’t shift

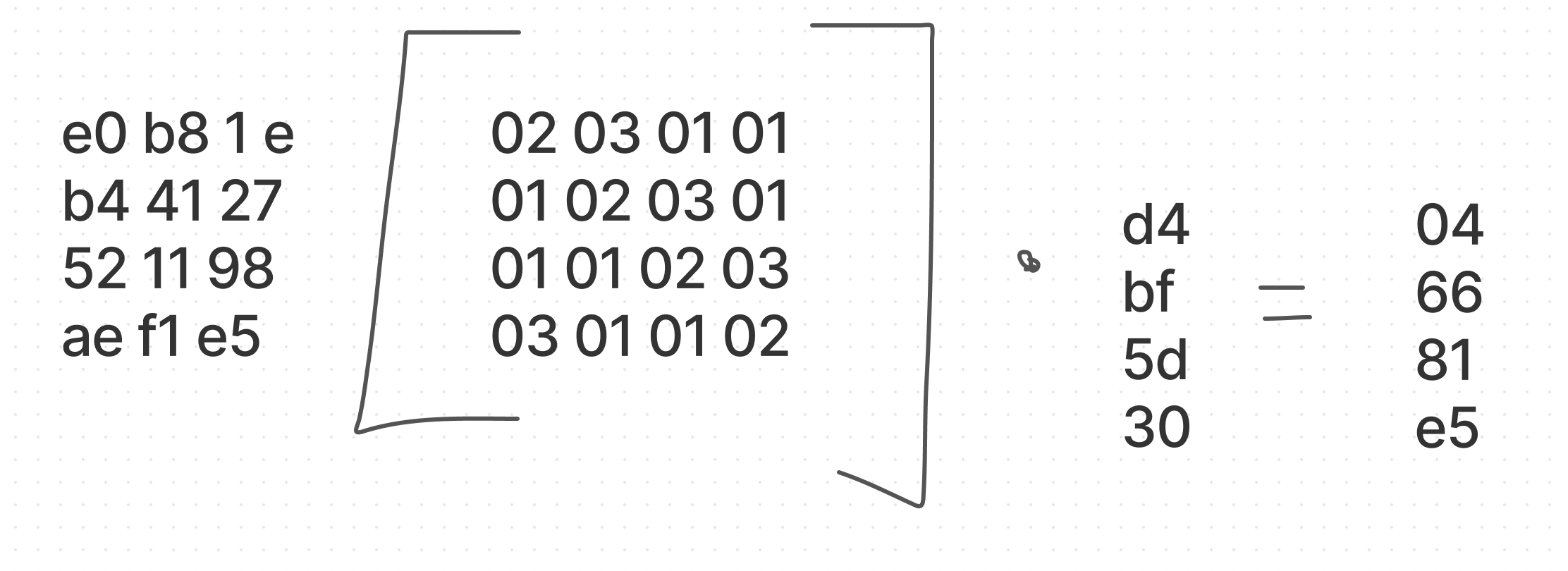
2nd row shfits over by 1 byte

3rd row shifts by 2 bytes

4th row shifts by 3 bytes

**3- MixColumn**

The four numbers of one column are moduled multipled in Rihandale’s Galois Field by a given matrix. Essentilly just matrix multiplication. One column x One row = the first number of the first column of output and so on.



**4 – Add Round Key**

XOR each column of the input with a each column of the round key.

**Example**: 1st column is XORed with 1st colmun of round key, 2nd Column is XORed with 2nd Column of Round key until the entire box has been XORed for our new output.

5- **Final Output**

**---------------------------------------------------------------------------------------------------------------------------------------**

**Key Scheduling:**

The epanded key can be seen as an arrray of 32 bit words(columns), number from 0 to 43. The fist four columns ar filled with the given Cipher key.

Words in poistions that are a multiple of 4(w4, w8,….w40)

Are calcualted by:

A) applying the RotWord and Subtyes transformation to the previous word Wi –1 (Last column)

B.) XORing this result to the word 4 positions earlier wi-4, plus a round cosntant Rcon

Example first column is xored by the 4th column to produce the 5th column, then you xor the 2nd column with the newly produced 5th column to produce the 6, etc...