

# MATH 314 Spring 2018 - Class Notes

4/9/2018

Scribe: Alex Goldberg

**Summary:** During today's class we went over how decryption of AES works. A demo of this was shown by Dr. McNew on CoCalc and is available in the Handouts folder called 'Simplified-AES'.

## Notes:

How does AES decryption work?

- If Bob is going to decrypt the message he first needs to compute the round keys from the master key in the same way Alice did for encryption.

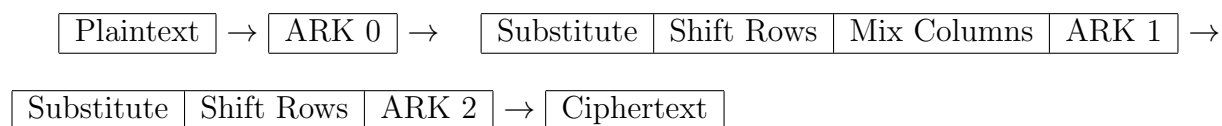
## Recall Mixed Columns:

- Matrix  $M$  entries in a  $\mathbb{F}_{16}$  multiply on the left by the encryption matrix  $E = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$
- The result is  $E \times M$ .

## Inverse Matrix Columns:

- We multiply on the left by the decryption matrix  $D = E^{-1}(\text{mod } x^4 + x + 1)$
- $D \times M = \text{Output of Mix Columns}$

## S-AES Encryption:



## S-AES Decryption:

