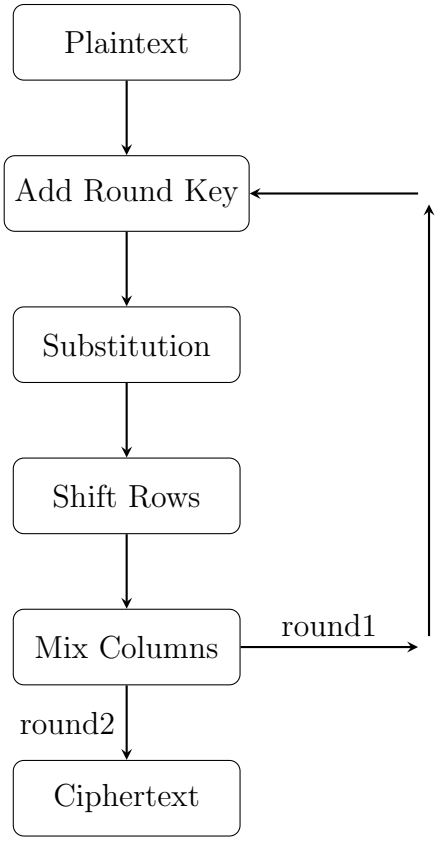
MATH 314 - Class Notes

04/13/2016

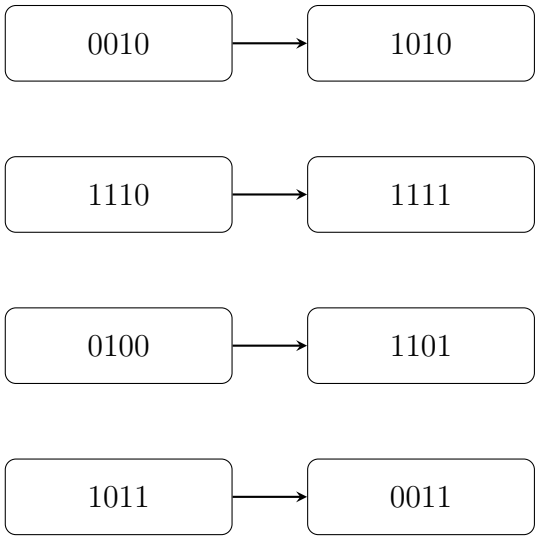
Scribe: Stephen Smith

Summary: This class served as the continuation of the SAES section. In the beginning, we finished an SAES example. Next, we looked at an example of using SAGE's SAES module. Finally, we were given a worksheet in which we did an SAES example by hand.

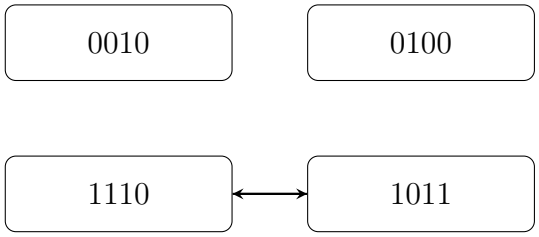
Notes: Flow of SAES:



Part 1 - Our Example: We started off at the end of round 1, with `0010 1110 0100 1011`. So we continue on with substitution.



So, we have `1010 1111 1101 0011`. Next, we will do the Shift Rows and Mix Columns steps. We start by writing our string down the columns of a matrix. Then, we swap the bottom two cells.



This leaves us with `1010 0011 1101 1111`. Finally, we xor this with our round key for round 2: `1000 0111 1010 1111`.

```
    1010 0011 1101 1111
⊕   1000 0111 1010 1111
-------------------------
    0010 0110 0111 0000
```

So our final ciphertext is: `0010 0110 0111 0000`.

Part 2 - Sage: See Simplified AES/Simplified AES.tex

Part 3 - Handout: See https://tigerweb.towson.edu/nmcnew/m314s17/homework.html