CIS 3362 - 10/8/21

1. Finish MixCols
2. Key Schedule
3. Quiz Notes
   - No extra notes, no calculator
   - 4 formula sheets given
   - Topics: bitwise ops, DES, AES

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} a3 & 17 & b6 & 12 \\ b4 & e3 & 47 & 34 \\ 78 & 42 & 92 & 56 \\ 26 & 98 & ee & 78 \end{pmatrix}$$

Mix Col Mat — Stk Matrix

Row 4 Col 3?

$03 \times b6 + 01 \times 47 + 01 \times 92 + 02 \times$ CC

47 92

$x^8 \equiv x^4 + x^3 + x + 1 \pmod{(x^8 + x^4 + x^3 + x + 1)}$

$3 \times b6$

$= (x+1)(x^7 + x^5 + x^4 + x^2 + x)$

0011 1011 0110

$= (x^8 + x^6 + x^5 + x^3 + x^2) + (x^7 + x^5 + x^4 + x^2 + x)$

$= (x^4 + x^3 + x + 1) + (x^6 + x^5 + x^3 + x^2) + (x^7 + x^5 + x^4 + x^2 + x)$

$= \boxed{x^7 + x^6 + 1}$

$3 \times b6 = 11 \times 10110110$

$$
\begin{array}{rl}
= & 10110110 \quad (1 \times b6) \\
 & +01101100 \quad (2 \times b6) \\
 & \quad 11011 \quad (x^8 \equiv x^4 + x^3 + x + 1) \\
\hline
 & 11000001 \quad (C1)
\end{array}
$$

$C7 \times e3$

$2 \times CC = 11001100 \times 2$

$= \$10011000$

$$
\begin{array}{r}
11011 \\
\hline
10000011 \ (83)
\end{array}
$$

$C1 + 47 + 92 + 83$

$86 + 11$

97

Example w/o overflow

$02 \times 73 = 01110011 \times 2$

$= 11100110 \ (e6)$

AES Key Schedule

Examples

w[17] = AB CD 79 3E
w[20] = 34 56 78 A4
w[21] = 9F 9B 01 9A

---

w[16] = 49 6A CB 73
w[19] = 87 65 4E FD
w[20] =

rot(w[19]) = 65 4E FD 87
sub(rot(w[19])) = 4D 2F 54 17 (from AES Sbox)
⊕ rcon[5] = 10 00 00 00

---

temp = 5D 2F 54 17
⊕ w[16] = 49 6A CB 73

---

14 45 9F 64

i=20/4

QUIZ

4 SHEETS (I GAVE)

1. Bitwise Ops (|, &, ^, >>, <<)
2. DES
   - Sboxes
   - IP
   - Key Schedule
3. AES
   - SubBytes
   - ShiftRows
   - MixCols (1 entry)
   - Key Schedule