CIS 3362 10/5/26

1) DES Key Schedule ✓
2) AES Math Background
3) GONE THURS-FRI
LEAVE WED EARLY

DES Key Schedule

1. $C_0 D_0 = PC\text{-}1(K)$
2. for $i = 1$ to 16:
   $C_i = LS_i(C_{i-1})$
   $D_i = LS_i(D_{i-1})$
   $K_i = PC\text{-}2(C_i D_i)$

C_0 = initial left 28 bits
D_0 = initial right 28 bits

$C_0 = [k_1 - k_7]$
$[k_9 - k_{15}]$
$[k_{17} - k_{23}]$
$[k_{25} - k_{31}]$

K is presented with 64 bits but the actual key is only 56 bits. Odd

$K = k_1\ k_2\ k_3\ k_4\ k_5\ k_6\ k_7\ k_8$ → Parity Bits
$k_9\ k_{10}$ ... k_{16}
⋮
$k_{57}\ k_{58}$ ... k_{64}

1011 0011 → parity bit!
0000 0100 → parity bit!

$C_0 D_0 = k_{57}\ k_{49}\ k_{41} \ldots k_{44}\ k_{36}\ k_{63}\ k_{55}\ k_{47} \ldots k_{12}\ k_4$

$LS_i(C_0)$, $LS_i(D_0)$ LS means cyclic left bitshift

$\longrightarrow$

$C_1 = k_{49}\ k_{41}\ k_{33} \ldots k_{44}\ k_{36}\ k_{57}$

$D_1 = k_{47}\ k_{39}\ k_{31} \ldots k_{12}\ k_4\ k_{63}$

PC-2: 14, 17, 11, 24, 1, 5, 3, 28

$k_{10}, k_{51}, k_{34}, k_{60}, k_{49}\ k_{17}\ k_{33}\ k_{57}$

16 round keys 48 bits each

$\frac{16 \times 48}{56}$ total bits used / # bits in key

$= \frac{16 \times 6}{7} \notin \mathbb{Z}$

AES is done is something known as a field in $GF(2^8)$. ???

↳ Polynomials with coefficients 0 or 1 of ~~upto degree~~ upto degree 7 because we do computations modulo a degree 8 polynomial.

AES polynomial IS $x^8 + x^4 + x^3 + x + 1$. Irreducible polynomial. There do not exist 2 polys f, g such that $f(x) \cdot g(x) = x^8 + x^4 + x^3 + x + 1$ and $f(x)$, $g(x)$ degree 1 or greater.

ADD : $(x^4 + x^3 + 1) + (x^6 + x^3 + x^2)$

$= x^6 + x^4 + \underline{\underline{2}}x^3 + x^2 + 1$ Compute all coeff mod 2

$\equiv \boxed{x^6 + x^4 + x^2 + 1}$

SUB SAME AS ADDITION

$(x^3 + x^2) - (x^2 + x)$

$= (x^3 + x^2) + (x^2 + x)$

MULT $(x^4 + x^3)(x^4 + x + 1)$

$= x^8 + x^5 + x^4$

$x^7 + x^4 + x^3$

$= x^8 + x^7 + x^3$

$\Longrightarrow$ OVERFLOW

Compute $(x^8 + x^7 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1)$

$$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^8 \qquad (1$$

$$- \; x^8 + x^4 + x^3 + x + 1$$

$x^4 + x^3 + x + 1$ Remainder

Thus $x^8 \bmod (x^8 + x^4 + x^3 + x + 1)$

$\equiv (x^4 + x^3 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$

So

Final Result is $(x^4 + x^3 + x + 1) + x^7 + x^3$

$\equiv \boxed{x^7 + x^4 + x + 1}$

$x^9 \equiv x \cdot x^8 \equiv x(x^4 + x^3 + x + 1)$

$\equiv x^5 + x^4 + x^2 + x \bmod (x^8 + x^4 + x^3 + x + 1)$