CIS 3362 10/2/2023

1. DES Key Schedule
2. Start AES

→ Key 56 bits but described as 64 bits w/ parity bits in positions 8, 16, 24, 32, 40, 48, 56, 64

1011 0110 (odd parity)
0000 1101
1010 1011
1111 1110
0001 0110
0110 1011
1000 0000
0001 0011

in HEX:
B60DABFE
166B8013

Key Schedule

1. $C_0 D_0 = PC\text{-}1(K)$, perm matrix
   (28 bits, 28 bits)

[57 49 41 33 ... 60 52 44 36] → C_0
[63 55 47 39 ... 28 20 12 4] → D_0

2. for $i = 1$ to 16
   $C_i = LS_i(C_{i-1})$
   $D_i = LS_i(D_{i-1})$

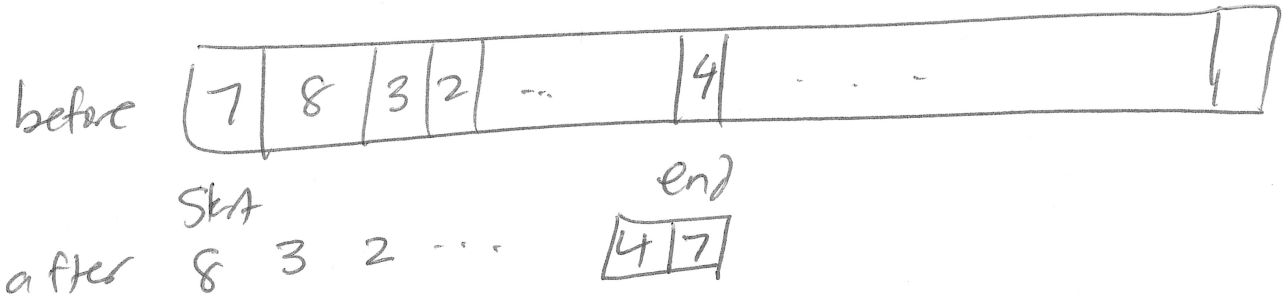
LS_i = left cyclic shift of either 1 or 2 bits. (Mostly 2, but for $LS_1 = LS_2 = LS_9 = LS_{16} = 1$.

$C_1 = [49\ 41\ 33 \ldots \quad 60\ 52\ 44\ 36\ 57]$

$D_1 = [55\ 47\ 39 \ldots \quad 28\ 20\ 12\ 4\ 63]$

$K_i = PC\text{-}2(C_i D_i)$, yet another perm matrix

leftShift



late 1990s DES challenge showed that brute force was possible so US Govt contest for a new private key encryption method

15 entries $\Longrightarrow$ 5 finalists

$\Longrightarrow$ Winner originally called Rijndahl - "Raindoll"

Joan Daemen Vincent Rijmen (Belgian)

Triple DES: $DES(DES(DES, K_1, P), K_2), K_1)$

AES

1) 3 specifications: 128 bits, 192 bits, 256 bits
both block, key size same. (much cleaner, also thought about future 3 version)

2) Modification in algorithm are relatively simple

3) Good security w/10 rounds for 128 bit

Algorithm

1. S = AddRoundKey(P, K_0)
2. for i = 1 to 9
   S = SubBytes(S)
   S = ShiftRows(S)
   S = MixCols(S) // hardest step ∄ non linear
   S = AddRoundKey(S, K_i)
3. S = SubBytes(S)
   S = ShiftRows(S)
   S = AddRoundKey(S, K_{10})
4. Return S

Stk Matrix for AES

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

Order of the bytes is $S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, \ldots, S_{35}$

↓↓↓↓ 128 bits = 16 bytes

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Stk Matrix

↓↓

K_{00}	K_{04}	K_{08}	K_{012}
K_{01}	K_{05}	K_{09}	K_{013}
K_{02}	K_{06}	K_{010}	K_{014}
K_{03}	K_{09}	K_{011}	K_{015}

(1) Add Round Key
XOR w/ the Round Key

(+)

(2) Shift Rows

(1) goes to

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

S_{00}	S_{01}	S_{02}	S_{03}
S_{11}	S_{12}	S_{13}	S_{10}
S_{22}	S_{23}	S_{20}	S_{21}
S_{33}	S_{30}	S_{31}	S_{32}