MATH 314 Spring 2018 - Class Notes

3/7/18

Scribe: Ethan Allen

Summary: This lesson began by briefly summarizing the history of the Data Encryption Standard (DES). We then went over a simplified version of DES and went through an example of it in action.

Feistel Cipher Consists of multiple rounds

Encryption:

$$\boxed{\mathrm{L}_{i+1}} = R_i$$

$$\boxed{\mathrm{R}_{i+1}} = f(R_i, k_i) \oplus L_i$$

Decryption:

$$\boxed{\mathrm{R}_i} = L_{i+1}$$

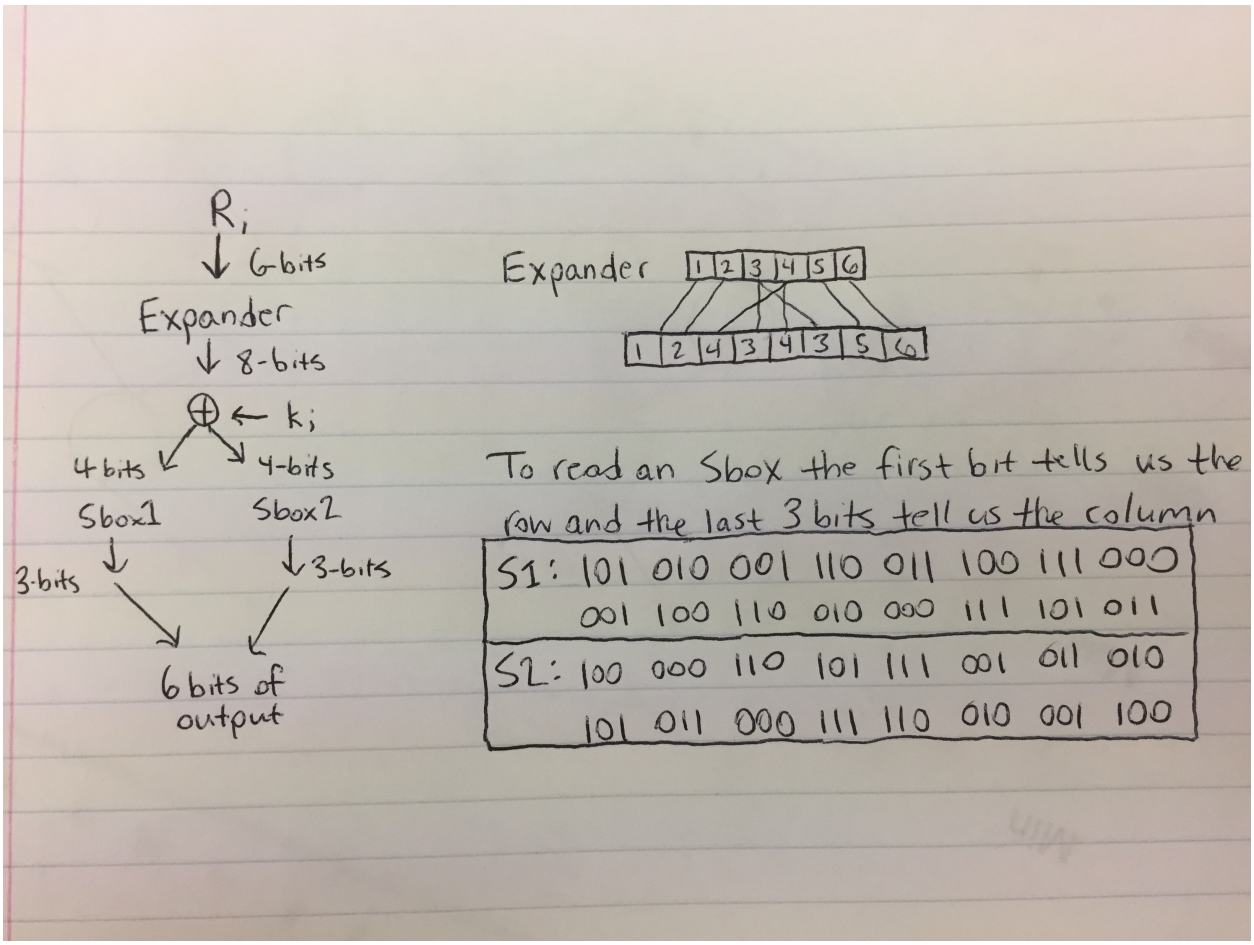
$$\boxed{\mathrm{L}_i} = f(L_{+1i}, k_i) \oplus R_i$$

Data Encryption Standard (DES)

- In 1972, NBS (existing today as NIST) put out a call for proposals for a national cryptosystem.
- IBM submitted a system called LUCIFER that they had developed
- NSA made some changes to LUCIFER but didn't explain why they made these changes
- This system was then adopted by MBS as the data encryption standard
- DES is a Feistel system using 16 rounds and 64-bit strings of plaintext
- We will talk about SDES (Simplified DES)

SDES Has 3 rounds with 16-bit messages

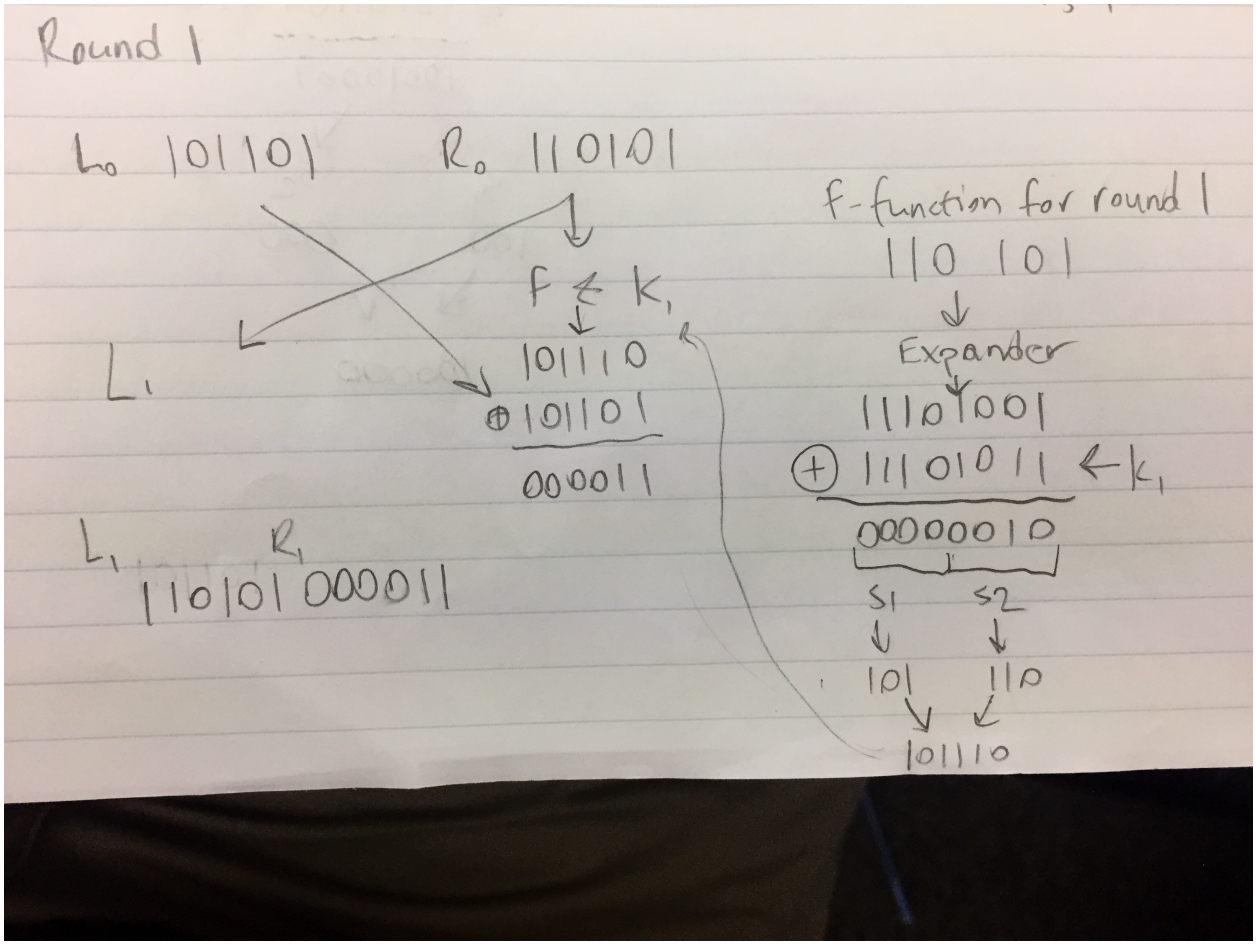
- Each round uses a Different Round Key
- Master key is 9-bits long–referred to as "k"
- Round key for round "i" is the 8-bits starting at bit "i" in k (and wrapping around if necessary)

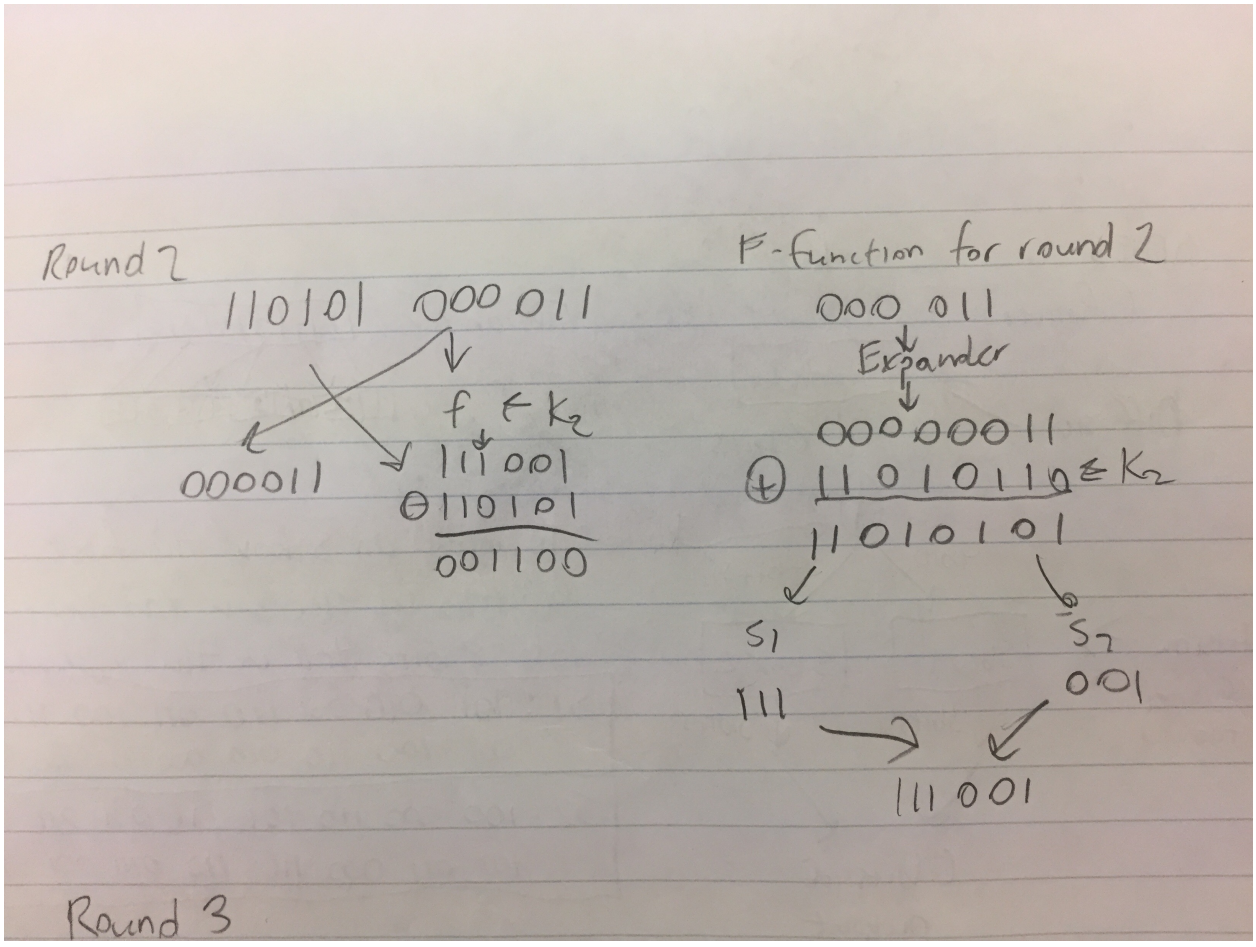


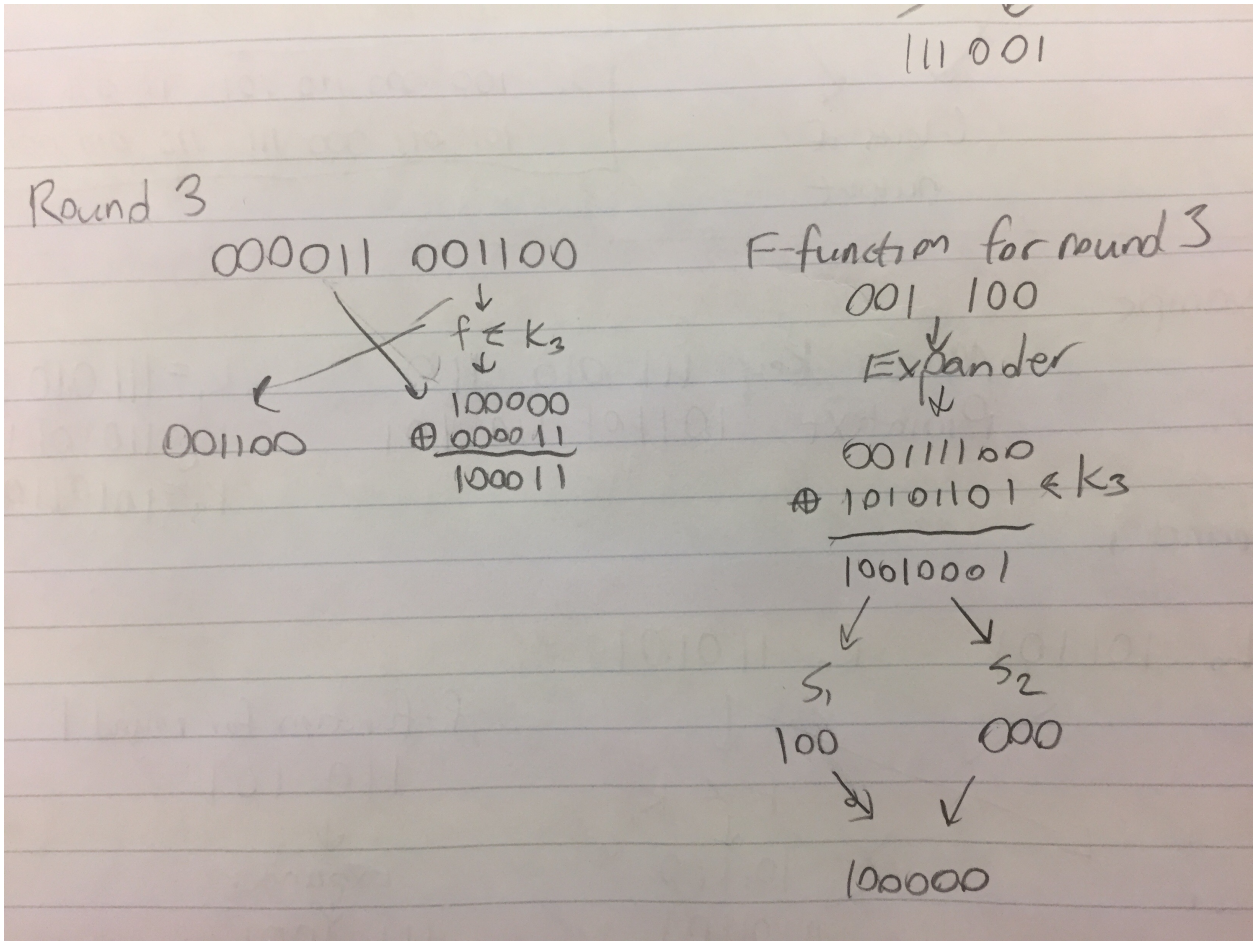
ABOVE: F-function for SDES

SDES Example

Master Key: 111 010 110
Plaintext: 101101 110 101
K1 = 111 000 11
K2 = 110 101 10
K1 = 101 011 01

(1).jpg 
Round 1
L0 10110
R0 11010
f ⇇ k1
L1
101110
⊕ 101101
000011
L1 R1
110101 000011
f-function for round 1
1101 01
Expander
11101001
⊕ 11101011 ← k1
00000010
S1 S2
101 110
101110

(4).jpg 
Round 2
110101 000011
000011
f ← k2
111001
⊕ 110101
001100
F-function for round 2
000 011
Expander
000000 11
⊕ 11010110 ← k2
11010101
S1
111
S2
001
111001
Round 3

(3).jpg 
111001
Round 3
000011 001100
f ∈ K3
100000
⊕ 000011
100011
001100
F-function for round 3
001 100
Expander
00111100
⊕ 10101101 ∈ K3
10010001
S1
S2
100
000
100000

Final Ciphertext: 001100 100011

To Decrypt: Swap left and right halves, then perform same steps as encryption but with reversed round key order: k3 then k2 then k1