MATH 314 Spring 2018 - Class Notes

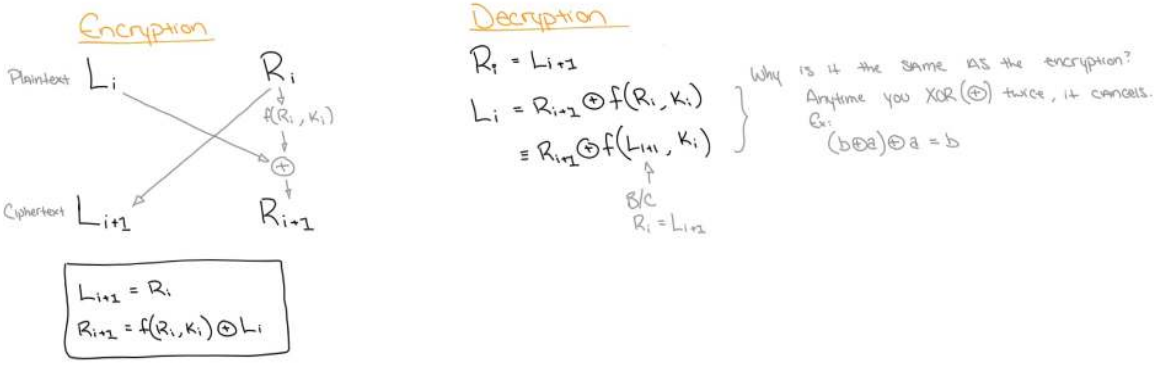
03/08/2010

Ronny Menendez

Summary:
Today we did a quick review of problem 4, from Mission 5, and we also reviewed one of the quiz questions from today's quiz. The review can be found at the end of the packet. Afterwards, we returned to Feistel Ciphers and we were able to discuss the encryption and decryption functions in more detail. Finally, we ended the class with SDES, a type of Feistel Cipher.

Feistel Ciphers

Alone, a Feistel Cipher does not stand as a cryptosystem. A Festel Cipher is more like a model, or receipe, for other systems to be made.



Pictured above is the general form for the encryption function and the decryption function.
L_i: left side of the plaintext R_i: right side of the plaintext
L_{i+1}: left side of ciphertext R_{i+1}: right side of ciphertext

Encryption
- To encrypt a plaintext, divide the text into 2 subparts: L_i and R_i
- L_{i+1} becomes R_i
- R_{i+1} becomes the result of $f(R_i, K_i) \oplus L_i$
  - $\oplus$ is the `XOR` operator
  - $f(R_i, K_i)$ is any function that rearranges R_i, more details found in SDES

Decryption
- R_i becomes L_{i+1}
- L_i becomes the result of $R_{i+1} \oplus f(L_{i+1}, K_i)$
  -Anytime you `XOR`($\oplus$) something twice, it cancels. (i.e. $(b \oplus a) \oplus a = b$)

Data Encryption Standard

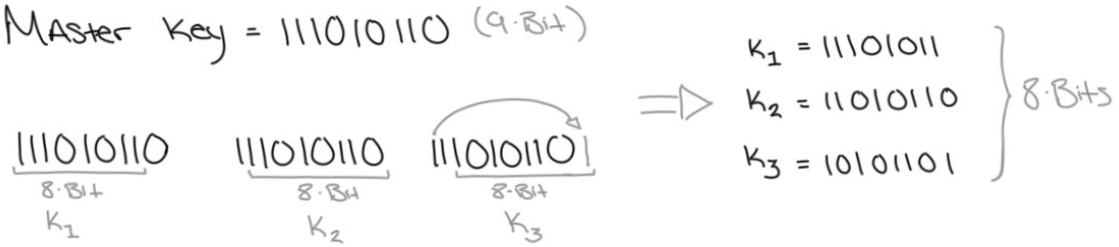
In 1972, NBS (NIST) put out a call for proposals for a national encryption standard. IBM submitted their system, called `LUCIFER` - a Feistel System. The NSA made some changes to `LUCIFER` but they did not explain why; however, the result of the changes became known as DES.

Idea of DES
- 16 Rounds
- 64 Bit Messages

As you can see, it's large. Instead, we will focus on SDES, or Simplified DES.

SDES - Simplified DES

- 3 Rounds
- 12 Bit Messages
- 9 Bit Master Key
  - However, the Round Key, K_i, is the 8 bits of the master key, starting with bit i and wrapping around if necessary.

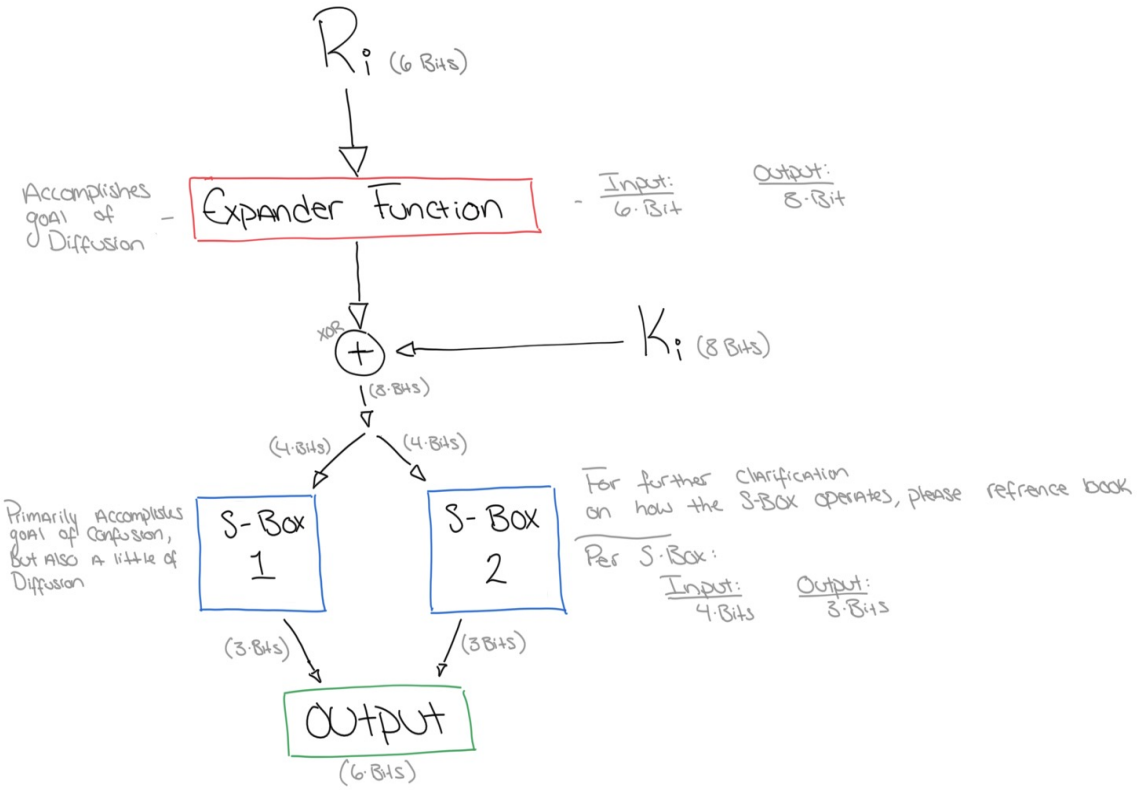


- f-function
  - Accomplishes diffusion and confusion
  - The following page will feature a diagram to better explain the idea

It should be the general goal of any good modern cryptosystem to include *confusion* and *diffusion*.

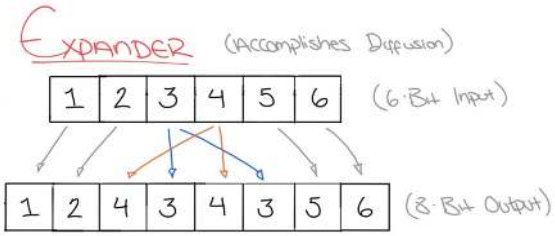
Confusion: Is defined as having a complex relation between the ciphertext and the key. In other words, the key should be hard to predict and every bit of the ciphertext should depend on every bit of the key.

Diffusion: Occurs when every bit of the ciphertext depends on every bit of the plaintext. Changing just one bit of the plaintext should flip about half of the ciphertext bits.



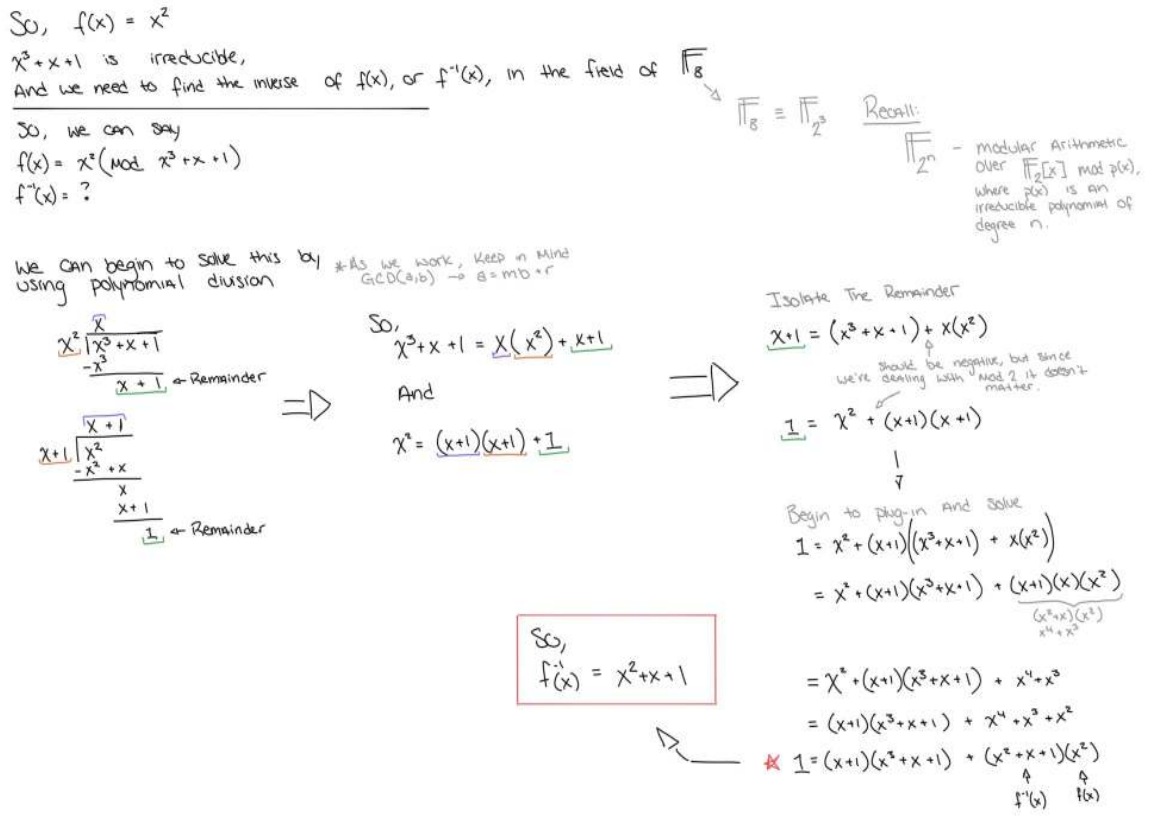
1. 6-bit R_i is fed into an Expander Function, which outputs 8-bits
2. R_i (8-bit) $\oplus$ K_i (8-bit)
3. The solution is split into two 4-bit parts - which are each sent to a separate `S-Box`
4. Each `S-Box` outputs 3-bits, which form a combined 6-bit final output

A Diagram to better explain the role of the Expander Function is found below:



Review: Let's begin with the problems we reviewed in class.

1. The first problem we reviewed was problem 4, from Mission 5:
   Use Euclid's algorithm to find the inverse of $f(x) = x^2$ in the field $\mathbb{F}_8$ with irreducible polynomial $x^3 + x + 1$.



2. The problem on the quiz asked us to compute 5^{19} $(mod 14)$