INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Homework 3 *September 9th, 2016*

1. Read the paper entitled *Block Cipher Modes of Operation from a Hardware implementation Perspective* written by Debrup Chakraborty and Francisco Rodríguez-Henríquez and do the following.

   a) Which are the most important block ciphers till now? Who design each of them and when?

   b) According to the paper, what is the definition of *block cipher*?

   c) What is a *round*? How many rounds does DES have ? How many rounds does AES have?

   d) What is the definition of *mode of operation*?

   e) Describe each mode of operation: ECB, CBC, OFB, CFB and counter mode (CTR)?

   f) What is the problem if use ECB?

   g) What are the advantages for each mode of operation?

   h) What is the main purpose of authenticated encryption?

2. Do a small research to know more about the cipher Lucifer, find biographical data about Horst Feistel. Explain what is the difference between Lucifer and DES.

3. Do a small research about Feistel networks, explain who invented them, using a diagram explain how they work and which block ciphers use them.

4. Find the following characteristics of AES: key size, block size, number of rounds, main operations, discover if AES uses a Feistel network.

Report

1. Write down a report in teams of 3 or 4 students. This report must be in Spanish and must contain the answers to the previous questions. Please include the references that you read. Cite the references in IEEE mode. Try not to make orthographic mistakes. You must send this report by email, in a pdf file. **Deadline to send this report is September 15, 2016(Thursday) before midday**.

2. Choose one of the following topics. To do it, **each team must send me an email next Wednesday (September 14)** indicating the name of each student in the team, and a topic of your choice. I will answer to you confirming your topic or I will give you a different one.

   - Lucifer and DES
   - Characteristics of block ciphers.
   - ECB, CBC
   - CTR, OFB, CFB
   - Authenticated Encryption

- Feistel Networks.

Make a video in English of 5 minutes to explain your topic.**You must upload your video to the cloud or youtube and send me the link by September 19th, before midday.**