VE475
Introduction to Cryptography

Assignment 3 (13/06/2017)

Manuel — UM-JI (Summer 2017)

Non-programming exercises:

- Write in a neat and legible handwriting, or use LaTeX
- Clearly explain the reasoning process
- Write in a complete style (subject, verb and object)

Progamming exercises:

- Write a README file for each program
- Upload an archive with all the programs onto Sakai

Ex. 1 — *Finite fields*

1. Show that X^2+1 is irreducible in $\mathbb{F}_3[X]$.
2. Why does the multiplicative inverse of $1+2X \bmod X^2+1$ exist in $\mathbb{F}_3[X]$?
3. Find the multiplicative inverse of $1+2X \bmod X^2+1$, in $\mathbb{F}_3[X]$.

Ex. 2 — *AES*

The goal of this exercise is to reshape the decryption of AES such that it has the same structure as encryption.

1. First we determine the inverse of each layer.
   a) Describe *InvShiftRows* the inverse operation of ShiftRows.
   b) What is the inverse of the layer AddRoundKey?
   c) Explain why the transformation *InvMixColumns* is given by the multiplication by the matrix

$$\begin{pmatrix} 00001110 & 00001011 & 00001101 & 00001001 \\ 00001001 & 00001110 & 00001011 & 00001101 \\ 00001101 & 00001001 & 00001110 & 00001011 \\ 00001011 & 00001101 & 00001001 & 00001110 \end{pmatrix}.$$

   We call *InvSubBytes* the lookup table inverse of SubBytes.
2. Describe the decryption process using the previous transformations.
3. Why can InvShiftRows and InvSubBytes be applied on reverse order?
4. Similarly we want to inverse the order of application of AddRoundKey and InvMixColumns.
   a) Why is it not possible to reverse the order of application of AddRoundKey and InvMixColumns?
   b) Calling the initial matrix $(a_{i,j})$, the MixColumns matrix $(m_{i,j})$, and the AddRoundKey matrix $(k_{i,j})$, what is the result of applying first MixColumns and then AddRoundKey?
   c) Show that the inverse operation is given by

$$(e_{i,j}) \to (m_{i,j})^{-1}(e_{i,j}) \oplus (m_{i,j})^{-1}(k_{i,j}).$$

   d) Define a new operations *InvAddRoundKey* such that "AddRounKey then InvMixColumns" can be replaced by "InvMixColumns then InvAddRoundKey".
5. Conclude on how to process the decryption.
6. What are the advantages of this strategy over simply reversing the order of application of the transformations?

Ex. 3 — *DES*

1. Research and explain how the DES cryptosystem works.
2. Quickly explain linear and differential cryptanalysis.
3. What is triple DES and why was it used instead of double DES?
4. Explain how passwords are stored on Unix systems? Is it a problem?

Hint: check `man passwd` and then follow the suggested man pages

Ex. 4 — *Programming*

In the AES, choose two layers to implement in C. The 128 bits should be looked at as an `unsigned char` pointer. Operations should be implemented using logical operators (and, or, and xor).

A bonus will be given for each extra layer implemented, and the generation of the S-Box. A big bonus will reward a complete implementation of the AES.