PRIMEIRA LISTA DE EXERCíCIOS

Criptografia e Segurança de redes – 01-2016

Disponibilizada em 03/04/2016 – A ser entregue em 26/04/2016

1. Write a program that implements the symmetric block cipher and decipher algorithm DES (Data Encryption Standard).

2. Write a program that implements the Extended Euclidean algorithm. Using this program find the multiplicative inverse of:
   a) 3041 mod 17331
   b) 213 mod 21753
   c) 548 mod 9571
   d) 24573 mod 68432

3. Write a program that implements a simple four-function calculator in GF(2^8) using modular polynomial arithmetic with the (irreducible) modulus polynomial given by $m(x) = x^8 + x^4 + x^3 + x + 1$. This is the same modulus polynomial used in the AES (Advanced Encryption Standard) algorithm. The four functions should be addition, subtraction, multiplication and division (all in GF(2^8)).

   Remember that $\frac{a}{b} = a * b^{-1}$ and $b * b^{-1} \equiv 1 \mod m(x)$

   You must implement the calculator using modular polynomial arithmetic. The inputs and outputs should be integer numbers between 0 and 255 (inclusive). Examples:

   $56_{10} = 00111000_2$ corresponds to $x^5 + x^4 + x^3$
   $253_{10} = 11111101_2$ corresponds to $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

   You should use the internal binary representation to execute operations on polynomials.