MAC5723+330 - CRIPTO - 1a. Prova - abril 2007

1. Questão 1 (50%)

O algoritmo de chave secreta a seguir criptografa um bloco de 64 bits, como no DES. (a) Escrever a função inversa nesta pseudo-linguagem, e (b) demonstrar que a sua inversa é correta.

Os parâmetros $SBoxes, AuxiliaryKeys, rotateSchedule$, e $Nrounds$ são pré–definidos ou pré-calculados. L e R são de 32 bits. Cada elemento da matriz $SBoxes$ é de 32 bits. $Nrounds$ deve ser um múltiplo de 8. $[L$ and $\#FF]$ são os 8 bits à direita de L. $TROCA[L, R]$ significa trocar L com R. $RotateRight(L, a)$ significa deslocar L circularmente para a direita a bits.

```
L, R : int32;                                    // entrada de 64 bits
Nrounds, i : integer;                            // múltiplo de 8
Sboxes : array [1..Nrounds/8]
        of array [0..255] of int32;
AuxiliaryKeys : array [1..4] of int32;
rotateSchedule : array [1..8] :=
      [16, 16, 8, 8, 16, 16, 24, 24]
round, indice : integer
L := L xor AuxiliaryKeys[1];
R := R xor AuxiliaryKeys[2];
indice := 1;
for round := 1 to Nrounds do
   begin
   R := R xor Sboxes[indice][L and #FF];
   i := 1 + (round − 1) mod 8;
   L := RotateRight[L, rotateSchedule[i]];       // desloca circularm/
   TROCA[L, R];                                  // troca L com R
   if (round mod 8 = 0)
      then indice := indice + 1;
   end;
L := L xor AuxiliaryKeys[3];
R := R xor AuxiliaryKeys[4];                     // (L, R) saída de 64 bits
```

2. Questão 2 (50%)

O Algoritmo de Euclides estendido é como segue:

Entrada: inteiros $a > 0$ e $b > 0$.
Saída: $mdc(a, b)$ e inteiros u e v tais que $mdc(a, b) = u \times a + v \times b$

1. $u_{-2} \leftarrow 1; v_{-2} \leftarrow 0; u_{-1} \leftarrow 0; v_{-1} \leftarrow 1; x_{-2} \leftarrow a; x_{-1} \leftarrow b; i \leftarrow 0$ (note que $\boxed{x_i = u_i \times a + v_i \times b}$ para $i = -2$ e para $i = -1$)
2. **enquanto** $x_{i-1} \neq 0$ **faça**{

   2.1 $q_i \leftarrow$ quociente de x_{i-2}/x_{i-1};

   2.2 $x_i \leftarrow x_{i-2} \bmod x_{i-1}$;

   2.3 $u_i \leftarrow u_{i-2} - q_i \times u_{i-1}$;

   2.4 $v_i \leftarrow v_{i-2} - q_i \times v_{i-1}$;

   2.5 $i \leftarrow i + 1$;

   2.6 } /* fim-enquanto */
3. Resposta é x_{i-2} tal que $mdc(a, b) = x_{i-2} = u_{i-2} \times a + v_{i-2} \times b$. $\square$

Esta questão consiste em:
(a) Executar este Algoritmo para $a = 48, b = 31$, mostrando os valores intermediários de

i	x_{i-2}	x_{i-1}	q_i	$x_i \leftarrow x_{i-2} \bmod x_{i-1}$	u_i	v_i	$i + 1$

(b) Demonstrar que de fato o algoritmo calcula

1. $x_{i-2} = mdc(a, b)$ e
2. inteiros u e v tais que $mdc(a, b) = u \times a + v \times b$

FIM FIM FIM