MAC0336/5723 Criptografia para Segurança de Dados
Lista 1

Mateus Agostinho dos Anjos
NUSP: 9298191

Exercício 1.

Sabemos que:
Dada n informações $X = \{x_1, x_2, \dots, x_n\}$ ocorrendo com as respectivas probabilidades $p(x_1), p(x_2), \dots, p(x_n)$ a Entropia é definida pela fórmula:

$$E(X) = \sum_{j=1}^{n} p(x_j) \log_2(\frac{1}{p(x_j)})$$

1. Dados do enunciado:
   $p(x_1) = 1/16$
   $p(x_2) = 1/4$
   $p(x_3) = 1/16$
   $p(x_4) = 1/4$
   $p(x_5) = 1/4$
   $p(x_6) = 1/16$
   $p(x_7) = 1/16$
   Aplicando a fórmula aos dados do enunciado temos:

$$4 * \frac{1}{16} \log_2(\frac{1}{(1/16)}) + 3 * \frac{1}{4} \log_2(\frac{1}{(1/4)})$$

$$\frac{1}{4} \log_2(\frac{1}{(1/16)}) + \frac{3}{4} \log_2(\frac{1}{(1/4)})$$

$$\frac{1}{4} \log_2(16) + \frac{3}{4} \log_2(4)$$

$$\frac{1}{4} * 4 + \frac{3}{4} * 2$$

$$1 + \frac{3}{2}$$

$$\frac{5}{2}$$

Resposta: Entropia de $X = \frac{5}{2}$

2. Queremos demonstrar que, para $j = 1, 2, \ldots, n$, $max_j\lceil\log_2[\frac{1}{p(x_j)}]\rceil$ representa o comprimento suficiente de bits para codificar cada um dos $x_j : j = 1, 2, \ldots, n$

   Veja que para j = 1 temos:
$$max_1\lceil\log_2[\frac{1}{p(x_1)}]\rceil = 0$$
   Para j = 2 devemos selecionar o máximo dentre os 2 valores
$$\sum_{j=1}^{2} p(x_j)\log_2(\frac{1}{p(x_j)}) \leq \sum_{j=1}^{2} p(x_j) max_j(\log_2[\frac{1}{p(x_j)}])$$
   Do mesmo modo, para j = n, temos:
$$\sum_{j=1}^{n} p(x_j)\log_2(\frac{1}{p(x_j)}) \leq \sum_{j=1}^{n} p(x_j) max_j(\log_2[\frac{1}{p(x_j)}])$$
   Como o termo $max_j(\log_2[\frac{1}{p(x_j)}])$ é igual em todas as parcelas do somatório à direita da inegualdade, podemos colocá-lo em evidência, ficando com:
$$\sum_{j=1}^{n} p(x_j)\log_2(\frac{1}{p(x_j)}) \leq \underbrace{\left(\sum_{j=1}^{n} p(x_j)\right)}_{1} max_j(\log_2[\frac{1}{p(x_j)}])$$
$$\underbrace{\sum_{j=1}^{n} p(x_j)\log_2(\frac{1}{p(x_j)})}_{\text{Entropia}} \leq 1 * max_j(\log_2[\frac{1}{p(x_j)}])$$
   Como o valor da entropia é menor ou igual a $max_j\lceil\log_2[\frac{1}{p(x_j)}]\rceil$ ele é um valor suficientemente grande de bits para decodificar os n valores propostos em X. ∎

3. Do enunciado temos que:

   I. A função $log_2()$ é estritamente côncava.

   II. Se $f : \mathbb{R} \to \mathbb{R}$ é uma função contínua estritamente côncava no intervalo I, então

$$\sum_{i=1}^{n} a_i f(y_i) \leq f(\sum_{i=1}^{n} a_i y_i)$$

   onde, para $1 \leq i \leq n : a_i \in \mathbb{R}, a_i > 0$ e $\sum_{i=1}^{n} a_i = 1$

   Temos que as probabilidades $p(x_i) \in \mathbb{R}, p(x_i) > 0$ de $X = \{x_1, x_2, \ldots, x_n\}$ somam 1, portanto a_i, definido em II, será $p(x_i)$.
   Seja $f(y) = log_2(y)$ temos que $f(y)$ é uma função estritamente côncava no intervalo $[0, 1]$, pois, como visto em I, a função $log_2()$ é estritamente côncava.
   Portanto, vale que:

$$\sum_{i=1}^{n} p(x_i) log_2 y_i \leq log_2(\sum_{i=1}^{n} p(x_i) y_i)$$

   Tomando y_i como $\frac{1}{p(x_i)}$ temos:

$$\sum_{i=1}^{n} p(x_i) log_2(\frac{1}{p(x_i)}) \leq log_2(\sum_{i=1}^{n} \frac{p(x_i)}{p(x_i)})$$

$$\sum_{i=1}^{n} p(x_i) log_2(\frac{1}{p(x_i)}) \leq log_2(\sum_{i=1}^{n} 1)$$

$$\underbrace{\sum_{i=1}^{n} p(x_i) log_2(\frac{1}{p(x_i)})}_{\text{Entropia de X}} \leq log_2(n)$$

$\blacksquare$

4. Provamos que a entropia máxima é de $log_2 n$, portanto

$$\sum_{i=i}^{n} p(x_i) log_2(\frac{1}{p(x_i)}) \leq log_2 n$$

   Trabalhando com $log_2 n$ para achar cadidatos a $p(x_i)$:

$$log_2 n = log_2(\frac{1}{1/n})$$

   Veja que $p(x_i) = \frac{1}{n}$ é um cadidato, verificaremos se é suficiente:

$$\sum_{i=i}^{n} \frac{1}{n} log_2(\frac{1}{1/n}) = n * \frac{1}{n} log_2(\frac{1}{1/n}) = log_2 n$$

   Nosso cadidato nos levou a um valor máximo de entropia (valor provado no item 3). Portanto, um conjunto $X = \{x_1, x_2, \ldots, x_n\}$ tal que $\forall x_i \in X, p(x_i) = \frac{1}{n}$, nos leva a uma entropia de valor máximo.

Exercício 2.

Neste exercício mostraremos os passos das divisões da seguinte forma:
1. *Dividendo* = Polinômio a ser dividido no momento
2. *Divisor* = Polinômio que está dividindo
3. *Quociente* = Valor do quociente no término desta etapa
4. (*Alter. no Quociente da etapa anterior*) $\times$ *Divisor* = Polinômio a ser subtraído do Dividendo
5. *Resto* = Polinômio resultante da operação (linha 1 - linha 4)

1.

$$(B2)_{16} = (10110010)_2$$

$$(15)_{16} = (10101)_2$$

Polinômio $s(x) = x^7 + x^5 + x^4 + x$
Polinômio $t(x) = x^4 + x^2 + 1$

$$u(x) = s(x) \times t(x) = ((x^7 + x^5 + x^4 + x) \times (x^4 + x^2 + 1)) mod 2 = x^{11} + x^8 + x^6 + x^4 + x^3 + x$$

$$u(x) = x^{11} + x^8 + x^6 + x^4 + x^3 + x$$

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Etapas da Divisão ($\oplus$ definido como XOR):

$$Dividendo = x^{11} + x^8 + x^6 + x^4 + x^3 + x$$

$$Divisor = x^8 + x^4 + x^3 + x + 1$$

$$Quociente = x^3$$

$$x^3 \times Divisor = x^{11} + x^7 + x^6 + x^4 + x^3$$

$$Resto = x^8 + x^7 + x$$

$$Dividendo = x^8 + x^7 + x$$

$$Divisor = x^8 + x^4 + x^3 + x + 1$$

$$Quociente = x^3 + 1$$

$$1 \times Divisor = x^8 + x^4 + x^3 + x + 1$$

$$Resto = x^7 + x^4 + x^3 + 1$$

Resultados:

$$Quociente: \ q(x) = x^3 + 1$$

$$Resto: \ r(x) = x^7 + x^4 + x^3 + 1$$

2. Calculo de $r^{-1}(x)$ mod $m(x)$:
Do algoritmo de Euclides Estendido temos: $X \times a + Y \times b = mdc(X, Y)$
Adaptando para o nosso exercício ficamos com: $r(x) \times a + m(x) \times b = mdc(r(x), m(x))$, verificaremos que $mdc(r(x), m(x)) = 1$, portanto $a = r^{-1}(x)$
Passos da divisão:

$$Dividendo = x^8 + x^4 + x^3 + x + 1$$
$$Divisor = x^7 + x^4 + x^3 + 1$$
$$Quociente = x$$
$$x \times Divisor = x^8 + x^5 + x^4 + x$$
$$Resto = x^5 + x^3 + 1$$

$$Dividendo = x^7 + x^4 + x^3 + 1$$
$$Divisor = x^5 + x^3 + 1$$
$$Quociente = x^2 + 1$$
$$(x^2 + 1) \times Divisor = x^7 + x^3 + x^2 + 1$$
$$Resto = x^4 + x^2$$

$$Dividendo = x^5 + x^3 + 1$$
$$Divisor = x^4 + x^2$$
$$Quociente = x$$
$$x \times Divisor = x^5 + x^3$$
$$Resto = 1$$

$$Dividendo = x^4 + x^2$$
$$Divisor = 1$$
$$Quociente = x^4 + x^2$$
$$(x^4 + x^2) \times Divisor = x^4 + x^2$$
$$Resto = 0$$

Conferimos que $mdc(r(x), m(x)) = 1$, agora acharemos $r^{-1}(x)$
Como queremos $r(x) \times r^{-1}(x) = 1 \ mod \ m(x)$ vamos preencher a tabela do algoritmo de euclides estendido até o resto 1.

Resto	Quociente	a
$x^8+x^4+x^3+x+1$	$*$	0
$x^7+x^4+x^3+1$	$*$	1
x^5+x^3+1	x	x
x^4+x^2	x^2+1	x^3+x+1
1	x	x^4+x^2

A partir da tabela acima, verificamos que $r^{-1}(x) = x^4 + x^2$, portanto:

$$r^{-1}(x) \ mod \ m(x) = x^4 + x^2$$

3. Verificaremos que: $r^{-1}(x) \otimes r(x) = 1 \ mod \ m(x)$

$$U(x) = r^{-1}(x) \times r(x)$$
$$U(x) = (x^4 + x^2) \times (x^7 + x^4 + x^3 + 1)$$
$$U(x) = x^{11} + x^8 + x^7 + x^4 + x^9 + x^6 + x^5 + x^2$$

Reescrevendo $U(x)$ temos:

$$U(x) = x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2$$

Agora dividiremos $U(x)$ por $m(x)$ para calcular o quociente $Q(x)$ e o resto $R(x)$

$$Dividendo = x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2$$
$$Divisor = x^8 + x^4 + x^3 + x + 1$$
$$Quociente = x^3$$
$$x^3 \times Divisor = x^{11} + x^7 + x^6 + x^4 + x^3$$
$$Resto = x^9 + x^8 + x^5 + x^3 + x^2$$

$$Dividendo = x^9 + x^8 + x^5 + x^3 + x^2$$
$$Divisor = x^8 + x^4 + x^3 + x + 1$$
$$Quociente = x^3 + x$$
$$x \times Divisor = x^9 + x^5 + x^4 + x^2 + x$$
$$Resto = x^8 + x^4 + x^3 + x$$

$$Dividendo = x^8 + x^4 + x^3 + x$$
$$Divisor = x^8 + x^4 + x^3 + x + 1$$
$$Quociente = x^3 + x + 1$$
$$1 \times Divisor = x^8 + x^4 + x^3 + x + 1$$
$$Resto = 1$$

Portanto $Q(x) = x^3 + x + 1$ e $R(x) = 1$

Exercício 3.

1. $A(x)$ e $B(x)$ representado da seguinte forma:
   Para $V(x) = [a_3, a_2, a_1, a_0]$

$V(x)$
a_3
a_2
a_1
a_0

$A(x)$	B(x)
10110010	00010010
01010101	01111011
10000111	11000100
00111101	01100110

Na forma polinomial temos:

$$A(x) = \big((x^7{+}x^5{+}x^4{+}x)x^3\big){+}\big((x^6{+}x^4{+}x^2{+}1)x^2\big){+}\big((x^7{+}x^2{+}x{+}1)x\big){+}\big(x^5{+}x^4{+}x^3{+}x^2{+}1\big)$$

$$B(x) = \big((x^4{+}x)x^3\big){+}\big((x^6{+}x^5{+}x^4{+}x^3{+}x{+}1)x^2\big){+}\big((x^7{+}x^6{+}x^2)x\big){+}\big(x^6{+}x^5{+}x^2{+}x\big)$$

2. Agora temos: $C(x) = A(x) \times B(x)$ (abaixo já está calculado o mod $m(x)$ dos termos entre parênteses):
   $C(x) =$
   $(x^7 + x^5 + x^3 + x)x^6+$
   $(x^5 + x^4 + x^2 + x + 1)x^5+$
   $(x^7 + x^3 + x^2 + 1)x^5+$
   $(x^6 + x^5 + x^4 + x^2 + 1)x^4+$
   $(x^7 + x^4 + x^2)x^4+$
   $(x^7 + x^5 + x^4 + x^3 + x^2 + 1)x^4+$
   $(x^6 + x^3 + 1)x^3+$
   $(x^7 + x^6 + x^5 + x^4)x^3+$
   $(x^7 + x^5 + x^4 + x + 1)x^3+$
   $(x^7 + x^2 + x + 1)x^3+$
   $(x^5 + x^4 + x^2 + x + 1)x^2+$
   $(x^7 + x^3 + x + 1)x^2+$
   $(x^6 + x^5 + x^4 + 1)x^2+$
   $(x^7 + x^6 + x^5 + x)x+$
   $(x^7 + x^2)x+$
   $(x^7 + x^5 + x^4 + x^2 + x)$

Mostrando $C(x)$ com coeficientes em hexadecimal temos:
$C(x) = (AA)x^6 + (37)x^5 + (8D)x^5 + (75)x^4 + (94)x^4 + (BD)x^4 + (49)x^3 + (F0)x^3 + (B3)x^3 + (87)x^3 + (37)x^2 + (8B)x^2 + (71)x^2 + (E2)x + (84)x + (B6)$

3. Agora calcularemos o polinômio resto $R(x)$ resultante da divisão $C(x)/M(x)$ utilizando o resultado visto no livro (página 99).

$$(a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3+$$
$$(a_0b_2 + a_1b_1 + a_2b_0 + a_3b_3)x^2+$$
$$(a_0b_1 + a_1b_0 + a_2b_3 + a_3b_2)x+$$
$$a_0b_0 + a_1b_3 + a_2b_2 + a_3b_1$$

Ficamos com:

$$(x^7 + x^3 + x^2 + 1)x^3$$
$$(x^6 + x^5 + x^2 + x + 1)x^2$$
$$(x^7 + x^6 + x^4 + x^3 + x^2)x$$
$$(x^7 + x^6 + x^5 + x^3 + x)$$

Portanto:

$C(x)modM(x)$
$(8D)_{16}$
$(67)_{16}$
$(DC)_{16}$
$(EA)_{16}$

Exercício 4.

1. Temos

   $$Ax = (x^7+x^5+x^4+x)x^3+(x^6+x^4+x^2+1)x^2+(x^7+x^2+x+1)x+(x^5+x^4+x^3+x^2+1)$$

2. Agora $C(x) = A(x) \times c(x)$:
   $C(x) =$
   $(x^7 + x^6 + x^3 + x^2 + 1)x^6+$
   $(x^7 + x^5 + x^4 + x)x^5+$
   $(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)x^5+$
   $(x^7 + x^5 + x^4 + x)x^4+$
   $(x^6 + x^4 + x^2 + 1)x^4+$
   $(x^7 + x^4 + x)x^4+$
   $(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)x^3+$
   $(x^6 + x^4 + x^2 + 1)x^3+$
   $(x^7 + x^2 + x + 1)x^3+$
   $(x^6 + x^2 + x + 1)x^3+$
   $(x^7 + x^5 + x^3 + x)x^2+$
   $(x^7 + x^2 + x + 1)x^2+$
   $(x^5 + x^4 + x^3 + x^2 + 1)x^2+$
   $(x^4 + x^2 + 1)x+$
   $(x^5 + x^4 + x^3 + x^2 + 1)x+$
   $(x^6 + x^5 + x^4 + x^3 + x)$

   Em hexadecimal temos:
   $C(x) = (CD)x^6 + (B2)x^5 + (FF)x^5 + (B2)x^4 + (55)x^4 + (92)x^4 + (7F)x^3 + (55)x^3 + (87)x^3 + (47)x^3 + (AA)x^2 + (87)x^2 + (3D)x^2 + (15)x + (3D)x + (7A)$

3. Agora o cálculo de $B(x) = C(x)\%M(x)$:
   Usando a fórmula 2.c) da página 99 do livro chegamos em:

$B(x)$
$(EA)_{16}$
$(DD)_{16}$
$(65)_{16}$
$(0F)_{16}$

Agora vamos calcular a inversa de $MixColumns(B)$ reproduzindo as operações anteriores com $A(x) = EADD650F$ e substituindo $c(x)$ por $c^{-1}(x)$ esperando encontrar como resposta $B(x) = B255873D$

4.

$$Ax = (x^7+x^6+x^5+x^3+x^1)x^3+(x^7+x^6+x^4+x^3+x^2+1)x^2+(x^6+x^5+x^2+1)x+(x^3+x^2+x+1)$$

5. $C(x) =$
$(x^5 + x^4 + x^2)x^6+$
$(x^6 + x^5 + x^4 + x^3 + x^2 + x)x^5+$
$(x^7 + x^6 + x^3 + x^2 + x)x^5+$
$(x^7 + x^6 + x^5 + x^4 + x^3 + x + 1)x^4+$
$(x^5 + x^4 + x^2 + x)x^4+$
$(x^7 + x^5 + x^3 + x)x^4+$
$(x^6 + x^4 + x^3 + x + 1)x^3+$
$(x^6 + x^5 + x^3 + x^2 + x + 1)x^3+$
$(x^7 + x^6 + x^5 + x^3 + x^2 + x + 1)x^3+$
$(x^6 + x^5 + x^3 + 1)x^3+$
$(x^6 + x^3 + x)x^2+$
$(x^6 + x^5)x^2+$
$(x^6 + x^3 + x + 1)x^2+$
$(x^6)x+$
$(x^6 + x^5 + x^4 + x^2 + x + 1)x+$
$(x^6 + x^4 + x^3 + x)$

Em Hexadecimal temos: $C(x) = (34)x^6+(7E)x^5+(CE)x^5+(FB)x^4+(36)x^4+(AA)x^4+(5B)x^3 + (6F)x^3 + (EF)x^3 + (69)x^3 + (4A)x^2 + (60)x^2 + (4B)x^2 + (40)x + (77)x + (5A)$

6. Agora o cálculo de $B(x) = C(x)\%M(x)$:
Usando a fórmula 2.c) da página 99 do livro chegamos em:

$B(x)$
$(B2)_{16}$
$(55)_{16}$
$(87)_{16}$
$(3D)_{16}$

∎