**II.** Fie sursa S2={A, B}de memorie zero. Simbolurile sursei sunt emise cu probabilitaţile:

a) PA = 0.104 ; b) PA = 0.486

Se va analiza separat pentru cazurile a) si b) introducand in discutie redundanta sursei de mesaje.

Se considera sistemul secret de simpla substitutie in cazul in care lungimea mesajului interceptat este N=1, N=2 si N=3.

Se cere:

1. Reprezentarea grafica si matricea de zgomot a canalului de informatie asociat sistemului secret de simpla substitutie in doua situatii : (a) spatiul de intrare este *X* (spatiul mesajelor clare); (b) spatiul de intrare este *K* (spatiul cheilor).
2. Evaluati cantitatea de secret privind mesajele, H(X/Y) si cantitatea de secret privind cheile, H(K/Y). Se vor comenta rezultatele pe baza aşteptărilor teoretice.
3. Discutati posibilitatea aparitiei solutiei unice. Se va trasa cantitatea de secret HN(X/Y) ca functie de numarul  *N* de litere interceptate.

**a) PA = 0.104 PB = 0.896**

**1)Lungimea mesajului interceptat este N=1**

Y-spatiul criptogramelor

Y={A,B} =>card Y=2 criptograme

Y={y0,y1}

Sistemul secret de simpla substitutie => spatiul mesajelor clare (X) are acelasi numar de elemente ca spatiul criptogramelor (Y).

X={A,B} =>card X=2 mesaje

X={x0,x1}

Probabilitatile mesajelor de intrare P(X):

p[x0] = 0.1040000000000000

p[x1] = 0.8960000000000000

Deoarece sursa S2 emite 2 simboluri, spatiul cheilor e egal cu (numarul de simboluri)!, adica 2!=2 chei.

K=spatiul cheilor={k0,k1}=>card K=2 chei

|  |  |  |
| --- | --- | --- |
| K | A | B |
| K0 | A | B |
| K1 | B | A |

P(Ki)=1/2; i=0,1

**1a)spațiul de intrare e X(spațiul mesajelor clare)**

O imagine care conține linie, Font, diagramă, Interval

Conținutul generat de inteligența artificială poate fi incorect.

Matricea de zgomot (spatiul mesajelor) P(Y|X):

p[y0|x0] = 0.5000000000000000

p[y1|x0] = 0.5000000000000000

p[y0|x1] = 0.5000000000000000

p[y1|x1] = 0.5000000000000000

Matricea de zgomot:

|  |  |  |
| --- | --- | --- |
| p(yj/xi) | y0  A | y1  B |
| x0:A | P(k0) | P(k1) |
| x1:B | P(k1) | P(k0) |

|  |  |  |
| --- | --- | --- |
| p(yj/xi) | y0  A | y1  B |
| x0:A | 1/2 | 1/2 |
| x1:B | 1/2 | 1/2 |

**1b)spațiul de intrare e K(spațiul cheilor)**

O imagine care conține text, Font, linie, diagramă

Conținutul generat de inteligența artificială poate fi incorect.

Matricea de zgomot (spatiul cheilor): P(Y|K)

p[y0|k0] = 0.1040000000000000

p[y0|k1] = 0.8960000000000000

p[y1|k0] = 0.8960000000000000

p[y1|k1] = 0.1040000000000000

|  |  |  |
| --- | --- | --- |
| p(yj/ki) | y0  A | y1  B |
| K0:AB | 0.104 | 0.896 |
| K1:BA | 0.896 | 0.104 |

Matricea de zgomot:

|  |  |  |
| --- | --- | --- |
| p(yj/ki) | y0  A | y1  B |
| K0:AB | P(x0) | P(x1) |
| K1:BA | P(x1) | P(x0) |

**2) Cantitatea de secret pe spatiul mesajelor: H(X|Y):**

Probabilitatile criptogramelor (spatiul mesajelor) P(Y):

p[y0] = 0.5000000000000000

p[y1] = 0.5000000000000000

Matricea probabilitatilor aposteriori (spatiul mesajelor) P(X|Y):

p[x0|y0] = 0.1040000000000000

p[x0|y1] = 0.1040000000000000

p[x1|y0] = 0.8960000000000000

p[x1|y1] = 0.8960000000000000

|  |  |  |
| --- | --- | --- |
| **p(xi/yj)** | **y0:A** | **y1:B** |
| **x0:A** | 0.104 | 0.104 |
| **x1:B** | 0.896 | 0.896 |
| H(X/yj) | 0.4815 | 0.4815 |

Valorile H(X|y):

H[X|y0] = 0.4815485438118001 [biti]

H[X|y1] = 0.4815485438118001 [biti]

Cantitatea de secret pe spatiul mesajelor: H(X|Y):

H[X|Y] = 0.4815485438118001 [biti]

**Cantitatea de secret pe spatiul cheilor H(K|Y):**

Probabilitatile criptogramelor (spatiul mesajelor) P(Y):

p[y0] = 0.5000000000000000

p[y1] = 0.5000000000000000

Matricea probabilitatilor aposteriori (spatiul cheilor) P(K|Y):

p[k0|y0] = 0.1040000000000000

p[k0|y1] = 0.8960000000000000

p[k1|y0] = 0.8960000000000000

p[k1|y1] = 0.1040000000000000

|  |  |  |
| --- | --- | --- |
| **p(ki/yj)** | **y0:A** | **y1:B** |
| **k0:AB** | 0.104 | 0.896 |
| **k1:BA** | 0.896 | 0.104 |
| H(K/yj) | 0.4815 | 0.4815 |

Valorile H(K|y):

H[K|y0] = 0.4815485438118001 [biti]

H[K|y1] = 0.4815485438118001 [biti]

Cantitatea de secret pe spatiul cheilor H(K|Y):

H[K|Y] = 0.4815485438118001 [biti]

1)card X=card Y=>SS inchis

2) Entropia pe spatiul mesajelor H(X) = 0.4815485438118001 [biti]

Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.4815485438118001 [biti]

I(X,Y)=H(X)-H(X|Y)= 0.4815485438118001-0.4815485438118001=0=>SS perfect

3) Entropia pe spatiul cheilor H(K)= 1.0000000000000000 [biti]

Cantitatea de secret pe spatiul cheilor H(K|Y) = 0.4815485438118001 [biti]

I(K,Y)=H(K)-H(K|Y)= 1.0000000000000000 -0.4815485438118001= 0.5184514561881999 !=0 =>SS nu e ideal

4) Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.4815485438118001 [biti] !=0 => Sistemul secret nu are solutie unica.