**2)Lungimea mesajului interceptat este N=2**

Y-spatiul criptogramelor

Y={AA,BB,AB,BA} =>card Y=4 criptograme

Y={y0,y1,y2,y3}

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

X={AA,BB,AB,BA} =>card X=4 mesaje

X={x0,x1,x2,x3}

Probabilitatile mesajelor de intrare P(X):

p[x0] = 0.0108160000000000

p[x1] = 0.8028160000000001

p[x2] = 0.0931840000000000

p[x3] = 0.0931840000000000

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, captură de ecran, 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[y2|x0] = 0.0000000000000000

p[y3|x0] = 0.0000000000000000

p[y0|x1] = 0.5000000000000000

p[y1|x1] = 0.5000000000000000

p[y2|x1] = 0.0000000000000000

p[y3|x1] = 0.0000000000000000

p[y0|x2] = 0.0000000000000000

p[y1|x2] = 0.0000000000000000

p[y2|x2] = 0.5000000000000000

p[y3|x2] = 0.5000000000000000

p[y0|x3] = 0.0000000000000000

p[y1|x3] = 0.0000000000000000

p[y2|x3] = 0.5000000000000000

p[y3|x3] = 0.5000000000000000

Matricea de zgomot:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p(yj/xi) | y0  AA | y1  BB | y2  AB | y3  BA |
| x0:AA | P(k0) | P(k1) | 0 | 0 |
| x1:BB | P(k1) | P(k0) | 0 | 0 |
| x2:AB | 0 | 0 | P(k0) | P(k1) |
| x3:BA | 0 | 0 | P(k1) | P(k0) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p(yj/xi) | y0  AA | y1  BB | y2  AB | y3  BA |
| x0:AA | 1/2 | 1/2 | 0 | 0 |
| x1:BB | 1/2 | 1/2 | 0 | 0 |
| x2:AB | 0 | 0 | 1/2 | 1/2 |
| x3:BA | 0 | 0 | 1/2 | 1/2 |

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

**O imagine care conține linie, diagramă, Interval, pantă

Conținutul generat de inteligența artificială poate fi incorect.**

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

p[y0|k0] = 0.0108160000000000

p[y0|k1] = 0.8028160000000001

p[y1|k0] = 0.8028160000000001

p[y1|k1] = 0.0108160000000000

p[y2|k0] = 0.0931840000000000

p[y2|k1] = 0.0931840000000000

p[y3|k0] = 0.0931840000000000

p[y3|k1] = 0.0931840000000000

Matricea de zgomot:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p(yj/ki) | y0  AA | y1  BB | y2  AB | y3  BA |
| K0:AB | P(x0) | P(x1) | P(x2) | P(x3) |
| K1:BA | P(x1) | P(x0) | P(x3) | P(x2) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p(yj/ki) | y0  AA | y1  AB | y2  BA | y3  BB |
| K0:AB | 0.0108 | 0.8028 | 0.0931 | 0.0931 |
| K1:BA | 0.8028 | 0.0108 | 0.0931 | 0.0931 |

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

Probabilitatile criptogramelor (spatiul mesajelor) P(Y):

p[y0] = 0.4068160000000001

p[y1] = 0.4068160000000001

p[y2] = 0.0931840000000000

p[y3] = 0.0931840000000000

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

p[x0|y0] = 0.0132934791158656

p[x0|y1] = 0.0132934791158656

p[x0|y2] = 0.0000000000000000

p[x0|y3] = 0.0000000000000000

p[x1|y0] = 0.9867065208841342

p[x1|y1] = 0.9867065208841342

p[x1|y2] = 0.0000000000000000

p[x1|y3] = 0.0000000000000000

p[x2|y0] = 0.0000000000000000

p[x2|y1] = 0.0000000000000000

p[x2|y2] = 0.5000000000000000

p[x2|y3] = 0.5000000000000000

p[x3|y0] = 0.0000000000000000

p[x3|y1] = 0.0000000000000000

p[x3|y2] = 0.5000000000000000

p[x3|y3] = 0.5000000000000000

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **p(xi/yj)** | **y0:AA** | **y1:BB** | **y2:AB** | **y3:BA** |
| **x0:AA** | 0.0132 | 0.0132 | 0 | 0 |
| **x1:BB** | 0.9867 | 0.9867 | 0 | 0 |
| **x2:AB** | 0 | 0 | 0.5 | 0.5 |
| **x3:BA** | 0 | 0 | 0.5 | 0.5 |
| H(X/yj) | 0.1019 | 0.1019 | 1 | 1 |

Valorile H(X|y):

H[X|y0] = 0.1019104763249953 [biti]

H[X|y1] = 0.1019104763249953 [biti]

H[X|y2] = 1.0000000000000000 [biti]

H[X|y3] = 1.0000000000000000 [biti]

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

H[X|Y] = 0.2692856246732586 [biti]

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

Probabilitatile criptogramelor (spatiul mesajelor) P(Y):

p[y0] = 0.4068160000000001

p[y1] = 0.4068160000000001

p[y2] = 0.0931840000000000

p[y3] = 0.0931840000000000

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

p[k0|y0] = 0.0132934791158656

p[k0|y1] = 0.9867065208841344

p[k0|y2] = 0.5000000000000000

p[k0|y3] = 0.5000000000000000

p[k1|y0] = 0.9867065208841344

p[k1|y1] = 0.0132934791158656

p[k1|y2] = 0.5000000000000000

p[k1|y3] = 0.5000000000000000

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **p(ki/yj)** | **y0:AA** | **y1:BB** | **y2:AB** | **y3:BA** |
| **k0:AB** | 0.0132 | 0.9867 | 0.5 | 0.5 |
| **k1:BA** | 0.9867 | 0.0132 | 0.5 | 0.5 |
| H(K/yj) | 0.1019 | 0.1019 | 1.0 | 1.0 |

Valorile H(K|y):

H[K|y0] = 0.1019104763249951 [biti]

H[K|y1] = 0.1019104763249951 [biti]

H[K|y2] = 1.0000000000000000 [biti]

H[K|y3] = 1.0000000000000000 [biti]

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

H[K|Y] = 0.2692856246732585 [biti]

1)card X=card Y=>SS inchis

2) Entropia pe spatiul mesajelor H(X) = 0.9630970876236003 [biti]

Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.2692856246732586 [biti]

I(X,Y)=H(X)-H(X|Y)= 0.9630970876236003 - 0.2692856246732586=0.6938114629503417 != 0=>SS nu este perfect

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

Cantitatea de secret pe spatiul cheilor H(K|Y) = 0.2692856246732585 [biti]

I(K,Y)=H(K)-H(K|Y)= 1.0000000000000000 - 0.2692856246732585 = 0.7307143753267415 !=0 =>SS nu e ideal

4) Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.2692856246732586 [biti] !=0 => Sistemul secret nu are solutie unica.