**3)Lungimea mesajului interceptat este N=3**

Y-spatiul criptogramelor

Y={AAA,BBB,AAB,BBA,ABA,BAB,ABB,BAA} =>card Y=8 criptograme

Y={y0,y1,y2,y3, y4,y5,y6,y7}

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

X={AAA,BBB,AAB,BBA,ABA,BAB,ABB,BAA} =>card X=8 mesaje

X={x0,x1,x2,x3, x4,x5,x6,x7}

Probabilitatile mesajelor de intrare P(X):

p[x0] = 0.0011248640000000

p[x1] = 0.7193231360000001

p[x2] = 0.0096911360000000

p[x3] = 0.0834928640000000

p[x4] = 0.0096911360000000

p[x5] = 0.0834928640000000

p[x6] = 0.0834928640000000

p[x7] = 0.0096911360000000

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 text, captură de ecran, Font, linie

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[y4|x0] = 0.0000000000000000

p[y5|x0] = 0.0000000000000000

p[y6|x0] = 0.0000000000000000

p[y7|x0] = 0.0000000000000000

p[y0|x1] = 0.5000000000000000

p[y1|x1] = 0.5000000000000000

p[y2|x1] = 0.0000000000000000

p[y3|x1] = 0.0000000000000000

p[y4|x1] = 0.0000000000000000

p[y5|x1] = 0.0000000000000000

p[y6|x1] = 0.0000000000000000

p[y7|x1] = 0.0000000000000000

p[y0|x2] = 0.0000000000000000

p[y1|x2] = 0.0000000000000000

p[y2|x2] = 0.5000000000000000

p[y3|x2] = 0.5000000000000000

p[y4|x2] = 0.0000000000000000

p[y5|x2] = 0.0000000000000000

p[y6|x2] = 0.0000000000000000

p[y7|x2] = 0.0000000000000000

p[y0|x3] = 0.0000000000000000

p[y1|x3] = 0.0000000000000000

p[y2|x3] = 0.5000000000000000

p[y3|x3] = 0.5000000000000000

p[y4|x3] = 0.0000000000000000

p[y5|x3] = 0.0000000000000000

p[y6|x3] = 0.0000000000000000

p[y7|x3] = 0.0000000000000000

p[y0|x4] = 0.0000000000000000

p[y1|x4] = 0.0000000000000000

p[y2|x4] = 0.0000000000000000

p[y3|x4] = 0.0000000000000000

p[y4|x4] = 0.5000000000000000

p[y5|x4] = 0.5000000000000000

p[y6|x4] = 0.0000000000000000

p[y7|x4] = 0.0000000000000000

p[y0|x5] = 0.0000000000000000

p[y1|x5] = 0.0000000000000000

p[y2|x5] = 0.0000000000000000

p[y3|x5] = 0.0000000000000000

p[y4|x5] = 0.5000000000000000

p[y5|x5] = 0.5000000000000000

p[y6|x5] = 0.0000000000000000

p[y7|x5] = 0.0000000000000000

p[y0|x6] = 0.0000000000000000

p[y1|x6] = 0.0000000000000000

p[y2|x6] = 0.0000000000000000

p[y3|x6] = 0.0000000000000000

p[y4|x6] = 0.0000000000000000

p[y5|x6] = 0.0000000000000000

p[y6|x6] = 0.5000000000000000

p[y7|x6] = 0.5000000000000000

p[y0|x7] = 0.0000000000000000

p[y1|x7] = 0.0000000000000000

p[y2|x7] = 0.0000000000000000

p[y3|x7] = 0.0000000000000000

p[y4|x7] = 0.0000000000000000

p[y5|x7] = 0.0000000000000000

p[y6|x7] = 0.5000000000000000

p[y7|x7] = 0.5000000000000000

Matricea de zgomot:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| p(yj/xi) | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| x0:AAA | P(k0) | P(k1) | 0 | 0 | 0 | 0 | 0 | 0 |
| x1:BBB | P(k1) | P(k0) | 0 | 0 | 0 | 0 | 0 | 0 |
| x2:AAB | 0 | 0 | P(k0) | P(k1) | 0 | 0 | 0 | 0 |
| x3:BBA | 0 | 0 | P(k1) | P(k0) | 0 | 0 | 0 | 0 |
| x4:ABA | 0 | 0 | 0 | 0 | P(k0) | P(k1) | 0 | 0 |
| x5:BAB | 0 | 0 | 0 | 0 | P(k1) | P(k0) | 0 | 0 |
| x6:ABB | 0 | 0 | 0 | 0 | 0 | 0 | P(k0) | P(k1) |
| x7:BAA | 0 | 0 | 0 | 0 | 0 | 0 | P(k1) | P(k0) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| p(yj/xi) | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| x0:AAA | 1/2 | 1/2 | 0 | 0 | 0 | 0 | 0 | 0 |
| x1:BBB | 1/2 | 1/2 | 0 | 0 | 0 | 0 | 0 | 0 |
| x2:AAB | 0 | 0 | 1/2 | 1/2 | 0 | 0 | 0 | 0 |
| x3:BBA | 0 | 0 | 1/2 | 1/2 | 0 | 0 | 0 | 0 |
| x4:ABA | 0 | 0 | 0 | 0 | 1/2 | 1/2 | 0 | 0 |
| x5:BAB | 0 | 0 | 0 | 0 | 1/2 | 1/2 | 0 | 0 |
| x6:ABB | 0 | 0 | 0 | 0 | 0 | 0 | 1/2 | 1/2 |
| x7:BAA | 0 | 0 | 0 | 0 | 0 | 0 | 1/2 | 1/2 |

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

**O imagine care conține text, captură de ecran, linie, diagramă

Conținutul generat de inteligența artificială poate fi incorect.**

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

p[y0|k0] = 0.0011248640000000

p[y0|k1] = 0.7193231360000001

p[y1|k0] = 0.7193231360000001

p[y1|k1] = 0.0011248640000000

p[y2|k0] = 0.0096911360000000

p[y2|k1] = 0.0834928640000000

p[y3|k0] = 0.0834928640000000

p[y3|k1] = 0.0096911360000000

p[y4|k0] = 0.0096911360000000

p[y4|k1] = 0.0834928640000000

p[y5|k0] = 0.0834928640000000

p[y5|k1] = 0.0096911360000000

p[y6|k0] = 0.0834928640000000

p[y6|k1] = 0.0096911360000000

p[y7|k0] = 0.0096911360000000

p[y7|k1] = 0.0834928640000000

Matricea de zgomot:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| p(yj/ki) | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| K0:AB | P(x0) | P(x1) | P(x2) | P(x3) | P(x4) | P(x5) | P(x6) | P(x7) |
| K1:BA | P(x1) | P(x0) | P(x3) | P(x2) | P(x5) | P(x4) | P(x7) | P(x6) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| p(yj/ki) | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| K0:AB | 0.0011 | 0.7193 | 0.0096 | 0.0834 | 0.0096 | 0.0834 | 0.0834 | 0.0096 |
| K1:BA | 0.7193 | 0.0011 | 0.0834 | 0.0096 | 0.0834 | 0.0096 | 0.0096 | 0.0834 |

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

Probabilitatile criptogramelor (spatiul mesajelor) P(Y):

p[y0] = 0.3602240000000000

p[y1] = 0.3602240000000000

p[y2] = 0.0465920000000000

p[y3] = 0.0465920000000000

p[y4] = 0.0465920000000000

p[y5] = 0.0465920000000000

p[y6] = 0.0465920000000000

p[y7] = 0.0465920000000000

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

p[x0|y0] = 0.0015613396109088

p[x0|y1] = 0.0015613396109088

p[x0|y2] = 0.0000000000000000

p[x0|y3] = 0.0000000000000000

p[x0|y4] = 0.0000000000000000

p[x0|y5] = 0.0000000000000000

p[x0|y6] = 0.0000000000000000

p[x0|y7] = 0.0000000000000000

p[x1|y0] = 0.9984386603890912

p[x1|y1] = 0.9984386603890912

p[x1|y2] = 0.0000000000000000

p[x1|y3] = 0.0000000000000000

p[x1|y4] = 0.0000000000000000

p[x1|y5] = 0.0000000000000000

p[x1|y6] = 0.0000000000000000

p[x1|y7] = 0.0000000000000000

p[x2|y0] = 0.0000000000000000

p[x2|y1] = 0.0000000000000000

p[x2|y2] = 0.1040000000000000

p[x2|y3] = 0.1040000000000000

p[x2|y4] = 0.0000000000000000

p[x2|y5] = 0.0000000000000000

p[x2|y6] = 0.0000000000000000

p[x2|y7] = 0.0000000000000000

p[x3|y0] = 0.0000000000000000

p[x3|y1] = 0.0000000000000000

p[x3|y2] = 0.8960000000000000

p[x3|y3] = 0.8960000000000000

p[x3|y4] = 0.0000000000000000

p[x3|y5] = 0.0000000000000000

p[x3|y6] = 0.0000000000000000

p[x3|y7] = 0.0000000000000000

p[x4|y0] = 0.0000000000000000

p[x4|y1] = 0.0000000000000000

p[x4|y2] = 0.0000000000000000

p[x4|y3] = 0.0000000000000000

p[x4|y4] = 0.1040000000000000

p[x4|y5] = 0.1040000000000000

p[x4|y6] = 0.0000000000000000

p[x4|y7] = 0.0000000000000000

p[x5|y0] = 0.0000000000000000

p[x5|y1] = 0.0000000000000000

p[x5|y2] = 0.0000000000000000

p[x5|y3] = 0.0000000000000000

p[x5|y4] = 0.8960000000000000

p[x5|y5] = 0.8960000000000000

p[x5|y6] = 0.0000000000000000

p[x5|y7] = 0.0000000000000000

p[x6|y0] = 0.0000000000000000

p[x6|y1] = 0.0000000000000000

p[x6|y2] = 0.0000000000000000

p[x6|y3] = 0.0000000000000000

p[x6|y4] = 0.0000000000000000

p[x6|y5] = 0.0000000000000000

p[x6|y6] = 0.8960000000000000

p[x6|y7] = 0.8960000000000000

p[x7|y0] = 0.0000000000000000

p[x7|y1] = 0.0000000000000000

p[x7|y2] = 0.0000000000000000

p[x7|y3] = 0.0000000000000000

p[x7|y4] = 0.0000000000000000

p[x7|y5] = 0.0000000000000000

p[x7|y6] = 0.1040000000000000

p[x7|y7] = 0.1040000000000000

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **p(xi/yj)** | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| x0:AAA | 0.0015 | 0.9984 | 0 | 0 | 0 | 0 | 0 | 0 |
| x1:BBB | 0.0015 | 0.9984 | 0 | 0 | 0 | 0 | 0 | 0 |
| x2:AAB | 0 | 0 | 0.1040 | 0.1040 | 0 | 0 | 0 | 0 |
| x3:BBA | 0 | 0 | 0.8960 | 0.8960 | 0 | 0 | 0 | 0 |
| x4:ABA | 0 | 0 | 0 | 0 | 0.1040 | 0.1040 | 0 | 0 |
| x5:BAB | 0 | 0 | 0 | 0 | 0.8960 | 0.8960 | 0 | 0 |
| x6:ABB | 0 | 0 | 0 | 0 | 0 | 0 | 0.8960 | 0.8960 |
| x7:BAA | 0 | 0 | 0 | 0 | 0 | 0 | 0.1040 | 0.1040 |
| H(X/yj) | 0.1680 | 0.1680 | 0.4815 | 0.4815 | 0.4815 | 0.4815 | 0.4815 | 0.4815 |

Valorile H(X|y):

H[X|y0] = 0.0168071465607281 [biti]

H[X|y1] = 0.0168071465607281 [biti]

H[X|y2] = 0.4815485438118001 [biti]

H[X|y3] = 0.4815485438118001 [biti]

H[X|y4] = 0.4815485438118001 [biti]

H[X|y5] = 0.4815485438118001 [biti]

H[X|y6] = 0.4815485438118001 [biti]

H[X|y7] = 0.4815485438118001 [biti]

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

H[X|Y] = 0.1467265336450598 [biti]

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

Probabilitatile criptogramelor (spatiul cheilor) P(Y):

p[y0] = 0.3602240000000000

p[y1] = 0.3602240000000000

p[y2] = 0.0465920000000000

p[y3] = 0.0465920000000000

p[y4] = 0.0465920000000000

p[y5] = 0.0465920000000000

p[y6] = 0.0465920000000000

p[y7] = 0.0465920000000000

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

p[k0|y0] = 0.0015613396109088

p[k0|y1] = 0.9984386603890912

p[k0|y2] = 0.1040000000000000

p[k0|y3] = 0.8960000000000000

p[k0|y4] = 0.1040000000000000

p[k0|y5] = 0.8960000000000000

p[k0|y6] = 0.8960000000000000

p[k0|y7] = 0.1040000000000000

p[k1|y0] = 0.9984386603890912

p[k1|y1] = 0.0015613396109088

p[k1|y2] = 0.8960000000000000

p[k1|y3] = 0.1040000000000000

p[k1|y4] = 0.8960000000000000

p[k1|y5] = 0.1040000000000000

p[k1|y6] = 0.1040000000000000

p[k1|y7] = 0.8960000000000000

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **p(ki/yj)** | y0  AAA | y1  BBB | y2  AAB | y3  BBA | y4  ABA | y5  BAB | y6  ABB | y7  BAA |
| **k0:AB** | 0.0015 | 0.9984 | 0.104 | 0.896 | 0.104 | 0.896 | 0.896 | 0.104 |
| **k1:BA** | 0.9984 | 0.0015 | 0.896 | 0.104 | 0.896 | 0.104 | 0.104 | 0.896 |
| H(K/yj) | 0.0168 | 0.0168 | 0.4815 | 0.4815 | 0.4815 | 0.4815 | 0.4815 | 0.4815 |

Valorile H(K|y):

H[K|y0] = 0.0168071465607281 [biti]

H[K|y1] = 0.0168071465607281 [biti]

H[K|y2] = 0.4815485438118001 [biti]

H[K|y3] = 0.4815485438118001 [biti]

H[K|y4] = 0.4815485438118001 [biti]

H[K|y5] = 0.4815485438118001 [biti]

H[K|y6] = 0.4815485438118001 [biti]

H[K|y7] = 0.4815485438118001 [biti]

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

H[K|Y] = 0.1467265336450598 [biti]

1)card X=card Y=>SS inchis

2) Entropia pe spatiul mesajelor H(X) = 1.4446456314354006 [biti]

Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.1467265336450598 [biti]

I(X,Y)=H(X)-H(X|Y)= 1.4446456314354006 - 0.1467265336450598=1.29791909779034 != 0=>SS nu este perfect

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

Cantitatea de secret pe spatiul cheilor H(K|Y) = 0.1467265336450598 [biti]

I(K,Y)=H(K)-H(K|Y)= 1.0000000000000000 - 0.1467265336450598= 0.8532734663549402 !=0 =>SS nu e ideal

4) Cantitatea de secreat pe spatiul mesajelor: H(X|Y) = 0.1467265336450598 [biti] !=0 => Sistemul secret nu are solutie unica.