Tema 5

Criptare

Pasul 1: Convertim mesajul "EXAMEN" în numere

Utilizăm următoarea convenție pentru conversia literelor în numere:

- A = 0
- B = 1
- ...
- Z = 25

Astfel, mesajul "EXAMEN" devine:

- E = 4
- X = 23
- A = 0
- M = 12
- E = 4
- N = 13

Scriem aceste numere în blocuri de câte două:

$(423),(012),(413)(423),(012),(413)$

Pasul 2: Aplicăm formula de criptare

Formula de criptare este: $Y=A\cdot X+B Y=A\cdot X+B$

Criptăm fiecare bloc:

1. Pentru primul bloc:

$X1=(423)X_1=(423)$
$Y1=(31145)\cdot(423)+(79)=(3\cdot4+11\cdot234\cdot4+5\cdot23)+(79)=(3\cdot4+11\cdot234\cdot4+5\cdot23)+(79)Y_1=(34115)\cdot(423)+(79)=(3\cdot4+11\cdot234\cdot4+5\cdot23)+(79)=(3\cdot4+11\cdot234\cdot4+5\cdot23)+(79)$
$=(12+25316+115)+(79)=(265131)+(79)=(272140)=(12+25316+115)+(79)=(265131)+(79)=(272140)$

$Y1\equiv(272140)(mod26)=(1210)Y_1\equiv(272140)(mod26)=(1210)$

2. Pentru al doilea bloc:

$X2=(012)X_2=(012)$
$Y2=(31145)\cdot(012)+(79)=(3\cdot0+11\cdot124\cdot0+5\cdot12)+(79)=(13260)+(79)=(13969)Y_2=(34115)\cdot(012)+(79)=(3\cdot0+11\cdot124\cdot0+5\cdot12)+(79)=(13260)+(79)=(13969)$
$Y2\equiv(13969)(mod26)=(917)Y_2\equiv(13969)(mod26)=(917)$

3. Pentru al treilea bloc:

$X3=(413)X_3=(413)$
$Y3=(31145)\cdot(413)+(79)=(3\cdot4+11\cdot134\cdot4+5\cdot13)+(79)=(4+14316+65)+(79)=(15081)+(79)=(15790)Y_3=(34115)\cdot(413)+(79)=(3\cdot4+11\cdot134\cdot4+5\cdot13)+(79)=(4+14316+65)+(79)=(15081)+(79)=(15790)$
$Y3\equiv(15790)(mod26)=(112)Y_3\equiv(15790)(mod26)=(112)$

Convertim rezultatele în litere:

- 12 -> M
- 10 -> K
- 9 -> J
- 17 -> R
- 1 -> B
- 12 -> M

Mesajul criptat este: **MKJRBM**

Decriptare

Pasul 1: Convertim mesajul criptat "SMOGKJECKGXX" în numere

$S=18,M=12,O=14,G=6,K=10,J=9,E=4,C=2,K=10,G=6,X=23,X=23S=18,M=12,O=14,G=6,K=10,J=9,E=4,C=2,K=10,G=6,X=23,X=23$

Scriem aceste numere în blocuri de câte două:

$(1812),(146),(109),(42),(106),(2323)(1812),(146),(109),(42),(106),(2323)$

Pasul 2: Inversăm matricea AA și găsim $A-1A^{-1}$

$A=(31145)A=(34115)$

Calculăm determinantul $\det(A)\det(A)$:

$\det(A)=3\cdot5-11\cdot4=15-44=-29\equiv-29+26\cdot2=23(\mathrm{mod}26)\det(A)=3\cdot5-11\cdot4=15-44=-29\equiv-29+26\cdot2=23(\mathrm{mod}26)$

Inversul lui 23 modulo 26 este un număr xx astfel încât $23x\equiv1(\mathrm{mod}26)23x\equiv1(\mathrm{mod}26)$. Acesta este 3 (pentru că $23\cdot3=69\equiv1(\mathrm{mod}26)23\cdot3=69\equiv1(\mathrm{mod}26)$).

Inversăm matricea AA:

$A-1=1\det(A)\cdot(5-11-43)\equiv3\cdot(515223)(\mathrm{mod}26)\equiv(1519149)(\mathrm{mod}26)A_{-1}=\det(A)1\cdot(5-4-113)\equiv3\cdot(522153)(\mathrm{mod}26)\equiv(1514199)(\mathrm{mod}26)$

Pasul 3: Decriptăm fiecare bloc

Formula de decriptare este: $X=A-1\cdot(Y-B)X=A_{-1}\cdot(Y-B)$

1. Pentru primul bloc:

$Y1=(1812)Y_1=(1812)$
$Y1-B=(1812)-(79)=(113)Y_1-B=(1812)-(79)=(113)$
$X1=(1519149)\cdot(113)\equiv(15\cdot11+19\cdot314\cdot11+9\cdot3)(\mathrm{mod}26)=(165+57154+27)(\mathrm{mod}26)=(222181)(\mathrm{mod}26)=(1423)X_1=(1514199)\cdot(113)\equiv(15\cdot11+19\cdot314\cdot11+9\cdot3)(\mathrm{mod}26)=(165+57154+27)(\mathrm{mod}26)=(222181)(\mathrm{mod}26)=(1423)$

2. Pentru al doilea bloc:

$Y2=(146)Y_2=(146)$
$Y2-B=(146)-(79)=(7-3)\equiv(723)Y_2-B=(146)-(79)=(7-3)\equiv(723)$
$X2=(1519149)\cdot(723)\equiv(15\cdot7+19\cdot2314\cdot7+9\cdot23)(\mathrm{mod}26)=(105+43798+207)(\mathrm{mod}26)=(542305)(\mathrm{mod}26)=(2019)X_2=(1514199)\cdot(723)\equiv(15\cdot7+19\cdot2314\cdot7+9\cdot23)(\mathrm{mod}26)=(105+43798+207)(\mathrm{mod}26)=(542305)(\mathrm{mod}26)=(2019)$

3. Pentru al treilea bloc:

$Y3=(109)Y_3=(109)$
$Y3-B=(109)-(79)=(30)Y_3-B=(109)-(79)=(30)$
$X3=(1519149)\cdot(30)\equiv(15\cdot3+19\cdot014\cdot3+9\cdot0)(\mathrm{mod}26)=(4542)(\mathrm{mod}26)=(1916)X_3=(1514199)\cdot(30)\equiv(15\cdot3+19\cdot014\cdot3+9\cdot0)(\mathrm{mod}26)=(4542)(\mathrm{mod}26)=(1916)$

4. Pentru al patrulea bloc:

$Y4=(42)Y_4=(42)$
$Y4-B=(42)-(79)=(-3-7)\equiv(2319)Y_4-B=(42)-(79)=(-3-7)\equiv(2319)$

$X4=(1519149)\cdot(2319)\equiv(15\cdot23+19\cdot1914\cdot23+9\cdot19)(mod26)=(345+361322+171)(mod26)=(706493)(mod26)=(425)$
$X_4=(1514199)\cdot(2319)\equiv(15\cdot23+19\cdot1914\cdot23+9\cdot19)(mod26)=(345+361322+171)(mod26)=(706493)(mod26)=(425)$

5. Pentru al cincilea bloc:

$Y5=(106)$
$Y_5=(106)$

$Y5-B=(106)-(79)=(3-3)\equiv(323)$
$Y_5-B=(106)-(79)=(3-3)\equiv(323)$

$X5=(1519149)\cdot(323)\equiv(15\cdot3+19\cdot2314\cdot3+9\cdot23)(mod26)=(45+43742+207)(mod26)=(482249)(mod26)=(1415)$
$X_5=(1514199)\cdot(323)\equiv(15\cdot3+19\cdot2314\cdot3+9\cdot23)(mod26)=(45+43742+207)(mod26)=(482249)(mod26)=(1415)$

6. Pentru al șaselea bloc:

$Y6=(2323)$
$Y_6=(2323)$

$Y6-B=(2323)-(79)=(1614)$
$Y_6-B=(2323)-(79)=(1614)$

$X6=(1519149)\cdot(1614)\equiv(15\cdot16+19\cdot1414\cdot16+9\cdot14)(mod26)=(240+266224+126)(mod26)=(506350)(mod26)=(1212)$
$X_6=(1514199)\cdot(1614)\equiv(15\cdot16+19\cdot1414\cdot16+9\cdot14)(mod26)=(240+266224+126)(mod26)=(506350)(mod26)=(1212)$

Convertim rezultatele în litere:

- 14 -> O
- 23 -> X
- 20 -> U
- 19 -> S
- 19 -> S
- 16 -> Q
- 4 -> E
- 25 -> Z
- 14 -> O
- 15 -> P
- 12 -> M
- 12 -> M

Mesajul decriptat este: **OXUSSQEZOPMM**