Tema 9

- Cheia publică: $\{34,51,58,11,39\}\{34,51,58,11,39\}$
- Cheia secretă: $(b=18,m=61)(b=18,m=61)$

Mesajul de criptat: "WHY"

Folosim următoarea mapare a caracterelor în numere:

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

Astfel, "WHY" devine:

- W = 22
- H = 7
- Y = 24

Fiecare caracter al mesajului se va transforma într-un vector binar de lungime 5 deoarece cheia publică are 5 elemente.

Vectori binari:

1. $W(22)W(22)$: Bin = 10110
2. $H(7)H(7)$: Bin = 00111
3. $Y(24)Y(24)$: Bin = 11000

Fiecare vector binar se cifrează folosind cheia publică.

Criptarea fiecărui caracter:

1. **W (10110):**

   $Suma=34\cdot1+51\cdot0+58\cdot1+11\cdot1+39\cdot0=34+0+58+11+0=103Suma=34\cdot1+51\cdot0+58\cdot1+11\cdot1+39\cdot0=34+0+58+11+0=103$

2. **H (00111):**

   $Suma=34\cdot0+51\cdot0+58\cdot1+11\cdot1+39\cdot1=0+0+58+11+39=108Suma=34\cdot0+51\cdot0+58\cdot1+11\cdot1+39\cdot1=0+0+58+11+39=108$

3. **Y (11000):**

$Suma=34\cdot1+51\cdot1+58\cdot0+11\cdot0+39\cdot0=34+51+0+0+0=85$$Suma=34\cdot1+51\cdot1+58\cdot0+11\cdot0+39\cdot0=34+51+0+0+0=85$

Mesajul criptat este: $103,108,85$$103,108,85$

Decriptare

Pentru a decripta mesajul cifrat $103,108,85$$103,108,85$, urmăm acești pași:

1. **Calculăm inversul lui $b$$b$ modulo $m$$m$:** Inversul lui $b=18$$b=18$ modulo $m=61$$m=61$ este un număr $b-1$$b^{-1}$ astfel încât $18\cdot b-1\equiv1(\mathrm{mod}61)$$18\cdot b^{-1}\equiv1(\mathrm{mod}61)$.

Folosim algoritmul extins al lui Euclid pentru a găsi inversul:

$61=3\cdot18+718=2\cdot7+47=1\cdot4+34=1\cdot3+13=3\cdot1+0$$61=3\cdot18+718=2\cdot7+47=1\cdot4+34=1\cdot3+13=3\cdot1+0$

Urmează înapoi:

$1=4-1\cdot33=7-1\cdot41=4-1\cdot(7-1\cdot4)=2\cdot4-1\cdot74=18-2\cdot71=2\cdot(18-2\cdot7)-1\cdot7=2\cdot18-5\cdot77=61-3\cdot181=2\cdot18-5\cdot(61-3\cdot18)=17\cdot18-5\cdot611=4-1\cdot33=7-1\cdot41=4-1\cdot(7-1\cdot4)=2\cdot4-1\cdot74=18-2\cdot71=2\cdot(18-2\cdot7)-1\cdot7=2\cdot18-5\cdot77=61-3\cdot181=2\cdot18-5\cdot(61-3\cdot18)=17\cdot18-5\cdot61$

Deci, $18-1\equiv17(\mathrm{mod}61)$$18^{-1}\equiv17(\mathrm{mod}61)$.

2. **Decriptăm fiecare sumă:**

$C\cdot b-1(\mathrm{mod}61)$$C\cdot b^{-1}(\mathrm{mod}61)$
$103\cdot17\mathrm{mod}\ 61=1751\mathrm{mod}\ 61=38$$103\cdot17\mathrm{mod}61=1751\mathrm{mod}61=38$
$108\cdot17\mathrm{mod}\ 61=1836\mathrm{mod}\ 61=7$$108\cdot17\mathrm{mod}61=1836\mathrm{mod}61=7$
$85\cdot17\mathrm{mod}\ 61=1445\mathrm{mod}\ 61=42$$85\cdot17\mathrm{mod}61=1445\mathrm{mod}61=42$

3. **Convertim rezultatele în binar folosind cheia secretă supercrescătoare $\{1,2,4,9,19\}$$\{1,2,4,9,19\}$:**

- **38:**

$38-19=1919-19=0\implies1$Rest: 0, folosit elementele: $19\implies10010\implies22(W)$$38-19=1919-19=0\Longrightarrow1$Rest: 0, folosit elementele: $19\Longrightarrow10010\Longrightarrow22(W)$

- **7:**

$$7-4=33-2=11-1=0 \implies 111 \implies 7(H)7-4=33-2=11-1=0\Longrightarrow111\Longrightarrow7(H)$$

- **42:**

$$42-19=2323-9=1414-4=1010-2=88-1=0 \implies 11000 \implies 24(Y)42-19=2323-9=1414-4=1010-2=88-1=0\Longrightarrow11000\Longrightarrow24(Y)$$

Mesajul decriptat este: "WHY"