|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Ă | Î | Ș | Ț |  |  |  |  |  |  |  |  |  |
| 26 | 27 | 28 | 29 |  |  |  |  |  |  |  |  |  |

**Sistemul de criptare Hill**

a1a2a3…ak

(a1a2a3…an) (a[n+1],a[n+2],…a[2n]) ….(a[mn+1],….ak), k se divide cu n, în ca contrar se completează cu o literă de frecvență joasă.

Numarul de caractere in alfabet

Legea de criptare:

E(x1,x2,…x[n])=) mod m≡ (b1,b2,…,b[n]) →(y1,y2,y3,…,y[n])

Legea de decriptare este:

D(y1,y2,…y[n])= mod m≡ (a1,a2,…,a[n]) →(x1,x2,x3,…,x[n])

unde, matricea ***q*** este inversa matricei ***f*** modulo ***m***. Detaliat, avem:

) mod m≡

Textul clar: **GUTIUMNICHITA**

Cheia: matrice de dimensiunea *n*

Cheia de criptare

*n*=3

6 24 1

13 11 10

20 17 15

Matricea inversa, m=29

|  |  |  |
| --- | --- | --- |
| 6 | 23 | 21 |
| 23 | 3 | 10 |
| 22 | 22 | 11 |

Pentru calcularea matricei inverse utilizati site-ul

<https://planetcalc.com/3324/>

Împărțim textul clar în secvențe de 3 caractere:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| xi | **G** | **U** | **T** | **I** | **U** | **M** | **N** | **I** | **C** | **H** | **I** | **T** | **A** | **Q** | **Q** |
| ai | 6 | 20 | 19 | 8 | 20 | 12 | 13 | 8 | 2 | 7 | 8 | 19 | 0 | 16 | 16 |

E(x1,x2,x3)= (a1a2a3) mod 29 – legea de criptare

E(GUT) ≡ ((6,20,19)( )) mod 29 ≡ (6∙6+20∙13+19∙20, 6∙24+20∙11+19∙17, 6∙1+20∙10+19∙15) mod 29≡(9,20,27)→**(JUÎ)**

E(IUM) ≡

E(NIC) ≡

E(HIT) ≡

E(AQQ) ≡

Textul criptat: **JUÎ…**

Decriptarea:

**JUÎ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| yi | **J** | **U** | **Î** |  |  |  |  |  |  |  |  |  |  |  |  |
| si | 9 | 20 | 27 |  |  |  |  |  |  |  |  |  |  |  |  |

Utilizam matricea inversa, m=29

|  |  |  |
| --- | --- | --- |
| 6 | 23 | 21 |
| 23 | 3 | 10 |
| 22 | 22 | 11 |

Legea de decriptare:

D(y1,y2,y3)= (s1,s2,s3) mod 29 – legea de criptare

D(JUÎ) ≡ ((9,20,27)( )) mod 29 ≡ (6, 20, 19)→**(GUT)**

**…**

Sarcina.

1. De criptat și decriptat până la final mesajul de mai sus aplicând Sistemul de criptare Hill. Matricea de criptare și decriptare poate fi calculată utilizând resursele site-ului <https://planetcalc.com/3324/>. Atenție! Este bine ca *n* să fie număr prim. Dacă un obțineți matricea inversă, atunci încercați să modificați matricea de criptare. În anexa 5 aveți un exemplu de calculare a inversei unei matrici modulo.
2. Scrieți un program care implementează criptarea cu ajutorul sistemului de criptare Hill. Se permite ca matricea de criptare și cea de decriptare să fie citite dintr-un fișier.
3. Opțional! Scrieți un program care implementează criptarea cu ajutorul sistemului de criptare Hill, unde matricea de criptare *M* se citește dint-un fișier, iar inversa *M*-1 se calculează direct în program. Se va lua în considerație și cazul când matricea *M* un are inversă (se poate întâmpla în cazul când *n* un este număr prim).