**Sistemul Cezar**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. Fie dat textul clar: **Ceata creaza o atmosfera misterioasa.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | **E** | **A** | **T** | **R** | **Z** | **O** | **M** | **S** | **F** | **I** |
| **2** | **4** | **0** | **19** | **17** | **25** | **14** | **12** | **18** | **5** | **8** |

1. Alegem cheia de criptare: **k=14**
2. Legea de criptare pentru sistemul de criptare Cezar este:

Ek(Tclar)=(Im(Tclar)+k) mod n; n-numărul de litere a alfabetului; n=26;

1. Criptarea:

Ek(C) ≡ (2+14) mod 26 ≡ 16 mod 26 ≡ 16 (Q)

Ek(E) ≡ (4+14) mod 26 ≡ 18 mod 26 ≡ 18 (S)

Ek(A) ≡ (0+14) mod 26 ≡ 14 mod 26 ≡ 14 (O)

Ek(T) ≡ (19+14) mod 26 ≡ 33 mod 26 ≡ 7 (H)

Ek(R) ≡ (17+14) mod 26 ≡ 31 mod 26 ≡ 5 (F)

Ek(Z) ≡ (25+14) mod 26 ≡ 39 mod 26 ≡ 13 (N)

Ek(O) ≡ (14+14) mod 26 ≡ 28 mod 26 ≡ 2 (C)

Ek(M) ≡ (12+14) mod 26 ≡ 26 mod 26 ≡ 0 (A)

Ek(S) ≡ (18+14) mod 26 ≡ 32 mod 26 ≡ 6 (G)

Ek(F) ≡ (5+14) mod 26 ≡ 19 mod 26 ≡ 19 (T)

Ek(I) ≡ (8+14) mod 26 ≡ 22 mod 26 ≡ 22 (W)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| cheia este k=14, care se adună cu fiecare număr modulo 26 | | | | | | | | | | | |
| **C** | **E** | **A** | **T** | **R** | **Z** | **O** | **M** | **S** | **F** | **I** |
| **2** | **4** | **0** | **19** | **17** | **25** | **14** | **12** | **18** | **5** | **8** |
| **Q** | **S** | **O** | **H** | **F** | **N** | **C** | **A** | **G** | **T** | **W** |
| **16** | **18** | **14** | **7** | **5** | **13** | **2** | **0** | **6** | **19** | **22** |

Text criptat: **QSOHO QFSONO C OHACGTSFO AWGHSFWCOGO**

1. Decriptarea:

**Dk(Tcriptat)=Im(Tcriptat)-k mod n;**

Text criptat: **QSOHO QFSONO C OHACGTSFO AWGHSFWCOG**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Q** | **S** | **O** | **H** | **F** | **N** | **C** | **A** | **G** | **T** | **W** |
| **16** | **18** | **14** | **7** | **5** | **13** | **2** | **0** | **6** | **19** | **22** |

Dk(Q) = 16-14 mod 26 ≡ 2 mod 26 ≡ 2 (C)

Dk(S) = 18-14 mod 26 ≡ 4 mod 26 ≡ 4 (E)

Dk(O) = 14-14 mod 26 ≡ 0 mod 26 ≡ 0 (A)

Dk(H) = 7-14 mod 26 ≡ -7 mod 26 ≡ -7+26 mod 26 ≡ 19 mod 26 ≡ 19(T)

Dk(F) = 5-14 mod 26 ≡ -9 mod 26 ≡ -9+26 mod 26 ≡ 17 mod 26 ≡ 17(R)

Dk(N) = 13-14 mod 26 ≡ -1+26 mod 26 ≡ 25 (Z)

Dk(C) = 2-14 mod 26 ≡ -12 mod 26 ≡ -12+26 mod 26 ≡ 14 mod 26 ≡ 14 (O)

Dk(A) = 0-14 mod 26 ≡ -14 mod 26 ≡ -14+26 mod 26 ≡ 12 mod 26 ≡ 12(M)

Dk(G) = 6-14 mod 26 ≡ -8 mod 26 ≡ -8+26 mod 26 ≡ 18 mod 26 ≡ 18 (S)

Dk(T) = 19-14 mod 26 ≡ 5 mod 26 ≡ 5 (5)

Dk(W) = 22-14 mod 26 ≡ 8 mod 26 ≡ 8 (I)

**Sistemul Cezar cu cheie**

Alegem un cuvânt sau o frază pe care o memorăm și o transmitem și destinatarului. De exemplu:

**Cheia: ECHIPA PROVEDENCE LAB**

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

1. 1. Fie dat textul clar: **Ceata creaza o atmosfera misterioasa.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | **E** | **A** | **T** | **R** | **Z** | **O** | **M** | **S** | **F** | **I** |
| **1** | **0** | **5** | **20** | **6** | **25** | **7** | **17** | **19** | **13** | **3** |

1. Alegem cheia de criptare: **k=14**
2. Legea de criptare pentru sistemul de criptare Cezar este:

Ek(Tclar)=Im(Tclar)+k mod n; n-numărul de litere a alfabetului; n=26;

Ek(C) ≡ (1+14) mod 26 ≡ 15 mod 26 ≡ 15 (J)

Ek(E) ≡ (0+14) mod 26 ≡ 14 mod 26 ≡ 14 (G)

Ek(A) ≡ (5+14) mod 26 ≡ 19 mod 26 ≡ 19 (S)

Ek(T) ≡ (20+14) mod 26 ≡ 34 mod 26 ≡ 8 (V)

Ek(R) ≡ (6+14) mod 20 ≡ 20 mod 26 ≡ 20 (T)

Ek(Z) ≡ (25+14) mod 26 ≡ 39 mod 26 ≡ 13 (F)

Ek(O) ≡ (7+14) mod 20 ≡ 21 mod 26 ≡ 21 (U)

Ek(M) ≡ (17+14) mod 26 ≡ 31 mod 26 ≡ 5 (A)

Ek(S) ≡ (19+14) mod 26 ≡ 33 mod 26 ≡ 7 (O)

Ek(F) ≡ (13+14) mod 26 ≡ 27 mod 26 ≡ 1 (C)

Ek(I) ≡ (3+14) mod 26 ≡ 17 mod 26 ≡ 17 (M)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C** | **E** | **A** | **T** | **R** | **Z** | **O** | **M** | **S** | **F** | **I** |
| **1** | **0** | **5** | **20** | **6** | **25** | **7** | **17** | **19** | **13** | **3** |
| **J** | **G** | **S** | **V** | **T** | **F** | **U** | **A** | **O** | **C** | **M** |
| **15** | **14** | **19** | **8** | **20** | **13** | **21** | **5** | **7** | **1** | **17** |

Text criptat: JGSVA JTGSFS U SVAUSCGTS AMOVGTMUSOS

1. Decriptarea:

Dk(Tcriptat)=Im(Tcriptat)-k mod n;

Text criptat: JGSVA JTGSFS U SVAUSCGTS AMOVGTMUSOS

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **J** | **G** | **S** | **V** | **T** | **F** | **U** | **A** | **O** | **C** | **M** |
| **15** | **14** | **19** | **8** | **20** | **13** | **21** | **5** | **7** | **1** | **17** |

Dk(J) = 15-14 mod 26 ≡ 1 mod 26 ≡ 1 (C)

Dk(G) = 14-14 mod 26 ≡ 0 mod 26 ≡ 0 (E)

Dk(S) = 19-14 mod 26 ≡ 5 mod 26 ≡ 5 (A)

Dk(V) = 8-14 mod 26 ≡ -6 mod 26 ≡ -6+26 mod 26 ≡ 20 mod 26 ≡ 20(T)

Dk(T) = 20-14 mod 26 ≡ 6 mod 26 ≡ 6 (R)

Dk(F) = 13-14 mod 26 ≡ -1+26 mod 26 ≡ 25 (Z)

Dk(U) = 21-14 mod 26 ≡ 7 mod 26 ≡ 7 (O)

Dk(A) = 5-14 mod 26 ≡ -9 mod 26 ≡ -9+26 mod 26 ≡ 17 mod 26 ≡ 17(M)

Dk(O) = 7-14 mod 26 ≡ -7 mod 26 ≡ -7+26 mod 26 ≡ 19 mod 26 ≡ 19(S)

Dk(C) = 1-14 mod 26 ≡ -13 mod 26 ≡ -13+26 mod 26 ≡ 13 mod 26 ≡ 13 (F)

Dk(M) = 17-14 mod 26 ≡ 3 mod 26 ≡ 3 (I)

Numărul de chei: 26!\*25=1\*2\*3\*...\*26\*25=10 082 286 528 165 140 889 600 000 000 > 1028

1 oră – 3600

1 zi – 3600\*24=86400

1 an – 365\*86400=31 536 000=3\*107

**Sistemul de criptare afin**

Numărul de caractere din alfabet

*n* caractere

(a,b),

(a,n)=1, a și n sunt reciproc prime, divizor comun egal cu 1

**E(M)=(a\*Im(M)+b) mod n** = Im(Q) –legea de criptare pentru sistemul afin, M – mesaj clar

Exemplu:

n=26

**Alegem doua numere: a=9, b=14**

**Atunci cheia de criptare va fi perechea (9,14).**

**Verificam** (9,26)=1,

Divizorii lui 9: **1**,3,9

Divizorii numărului 26: **1**,2,13,26

E(M)=(9\*Im(M)+14) mod 26≡ Im(Q)→Q

Utilizăm tabelul:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

**sau putem utiliza o frază cheie.**

**Mesaj clar: Ceata creaza o atmosfera misterioasa.**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **M** | **C** | **E** | **A** | **T** | **R** | **Z** | **O** | **M** | **S** | **F** | **I** |
| **Im(M)** | **2** | **4** | **0** | **19** | **17** | **25** | **14** | **12** | **18** | **5** | **8** |

E(M)=(9\*Im(M)+14) mod 26≡ Im(Q)→Q

E(C)=(9\*2+14) mod 26≡ 6 (G)

E(E)=(9\*4+14) mod 26 ≡ 24 (Y)

E(A)=(9\*0+14) mod 26 ≡ 14 (O)

E(T)=(9\*19+14) mod 26 ≡ 3(D)

E(R)=(9\*17+14) mod 26 ≡ 11 (L)

E(Z)=(9\*25+14) mod 26 ≡ 5 (F)

E(O)=(9\*14+14) mod 26 ≡ 10 (K)

E(M)=(9\*12+14) mod 26 ≡ 18 (S)

E(S)=(9\*18+14) mod 26 ≡ 20 (U)

E(F)=(9\*5+14) mod 26 ≡ 7 (H)

E(I)=(9\*8+14) mod 26 ≡ 8 (I)

Text criptat: GYODO GLYOFO K ODSKUHYLO SIUDYLIKOUO

DECRIPTAREA:

**D(Q) ≡ (Im(Q)-b+n)) mod n=Im(M)** →M – legea de decriptare

- inversul numărului *a* modulo *n*

. Acesta relatie este echivalenta cu ( se imparte la *n* fara rest.

*a*=9, există oricând dacă *n* este număr prim

Algoritmul lui Euclid extins (procedura Inv din anexa 2).

=3

Verificăm: 9\*3=27; 27 mod 26=1

**D(Q) ≡ (Im(Q)-14+26)) mod 26 ≡ 3(Im(Q)+12) mod 26**

Mesaj criptat: GYODO GLYOFO K ODSKUHYLO SIUDYLIKOUO

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Q** | **G** | **Y** | **O** | **D** | **L** | **F** | **K** | **S** | **U** | **H** | **I** |
| **Im(Q)** | **6** | **24** | **14** | **3** | **11** | **5** | **10** | **18** | **20** | **7** | **8** |

D(G)=(6+12) mod 26 ≡ 2 (**C**)

D(Y)=(24+12) mod 26 ≡ 4 (**E**)

D(O)=(14+12) mod 26 ≡ 0 (**A**)

D(D)=(3+12) mod 26 ≡ 19 (**T**)

D(L)=(11+12) mod 26 ≡ 17 (**R**)

D(F)=(5+12) mod 26 ≡ 25 (**Z**)

D(K)=(10+12) mod 26 ≡ 14 (**O**)

D(S)=(18+12) mod 26 ≡ 12 (**M**)

D(U)=(20+12) mod 26 ≡ 18 (**S**)

D(H)=(7+12) mod 26 ≡ 5 (**F**)

D(I)=(8+12) mod 26 ≡ 8 (**I**)

Am obținut textul clar: **Ceata creaza o atmosfera misterioasa.**

**Sistemul de criptare Polibios, *n*=26, a fost exclusă litera Q**

Cheia de criptare/decriptare este tabelul de mai jos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| A | E | C | H | I | P |
| B | A | R | O | V | D |
| C | N | L | B | F | G |
| D | J | K | M | S | T |
| E | U | W | X | Y | Z |

Și următoarea **Cheia: ECHIPA PROVEDENCE LAB**

Mesaj clar: **Ceata creaza o atmosfera misterioasa.**

Fiecărei litere i se pune în corespondență numele liniei și numele coloanei

C → linia C și coloana 1, deci C se criptează cu C1.

Mesaj criptat: A2A1B1D5B1 A2B2A1B1E5B1 B3 B1D5B3B3D4C4A1B2B1 D3A1D4D5A1B2A4B3B1D4B1

Decriptarea:

Avem textul criptat: A2A1B1D5B1 A2B2A1B1E5B1 B3 B1D5B3B3D4C4A1B2B1 D3A1D4D5A1B2A4B3B1D4B1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| A | E | C | H | I | P |
| B | A | R | O | V | D |
| C | N | L | B | F | G |
| D | J | K | M | S | T |
| E | U | W | X | Y | Z |

C1 – intersecția liniei C cu coloana 1: va fi litera **C.**

Mesaj clar: **Ceata creaza o atmosfera misterioasa.**

**Cifru cu permutare**

Fie dat textul clar: **Ceata creaza o atmosfera misterioasa.**

1. Alegem permutarea care va fi legea/cheia de criptare:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| 3 | 5 | 1 | 2 | 4 |

1. Criptarea: se împarte textul clar în secvențe a câte 5 litere (permutarea este formată din 5 elemente); în cazul în care, ultima secvență de litere nu este completă, atunci se adaugă litera care se utilizează cel mai rar în scrierea textelor clare.

**Ceata**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| C | E | A | T | A |
| A | T | C | A | E |

**–crea**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| - | C | R | E | A |
| R | E | - | A | C |

**za-o-**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| Z | A | - | O | - |
| - | O | Z | - | A |

**Atmos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| A | T | M | O | S |
| M | O | A | S | T |

**fera-**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| F | E | R | A | - |
| R | A | F | - | E |

**Miste**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| M | I | S | T | E |
| S | T | M | E | I |

**Rioas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| R | I | O | A | S |
| O | A | R | S | I |

**aQQQQ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| A | Q | Q | Q | Q |
| Q | Q | A | Q | Q |

Textul criptat:

ATCAERE-AC-OZ-AMOAS TRAF-ESTMEIOARSIQQAQQ

Decriptarea:

Creăm cheia de decriptare:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| 3 | 4 | 1 | 5 | 2 |

ATCAE RE-AC -OZ-A MOAST RAF-E STMEI OARSI QQAQQ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| A | T | C | A | E |
| C | E | A | T | A |
| 1 | 2 | 3 | 4 | 5 |
| R | E | - | A | C |
| - | C | R | E | A |
| 1 | 2 | 3 | 4 | 5 |
| - | O | Z | - | A |
| Z | A | - | O | - |
| 1 | 2 | 3 | 4 | 5 |
| M | O | A | S | T |
| A | T | M | O | S |
| 1 | 2 | 3 | 4 | 5 |
| R | A | F | - | E |
| F | E | R | A | - |
| 1 | 2 | 3 | 4 | 5 |
| S | T | M | E | I |
| M | I | S | T | E |
| 1 | 2 | 3 | 4 | 5 |
| O | A | R | S | I |
| R | I | O | A | S |
| 1 | 2 | 3 | 4 | 5 |
| Q | Q | A | Q | Q |
| A | Q | Q | Q | Q |

Textul clar: **Ceata creaza o atmosfera misterioasa**