**Sisteme de criptare cu chei fluide**

1. Sisteme de criptare cu chei fluide sincrone
2. Vigenere
3. În caliatate de cheie putem lua un șir de numere ilustre

De exemplu, șirul numerelor Fibbonacci

F(i)=F(i-1)+F(i-2), F(1)=F(2)=1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Fi | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 | 610 | 987 |
| Fi mod 26 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 8 | 3 | 11 | 14 | 25 | 13 | 12 | 25 |

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

Text clar: **CROITOR ANDREIA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | R | O | I | T | O | R | A | N | D | R | E | I | A |
| 2 | 17 | 14 | 8 | 19 | 14 | 17 | 0 | 13 | 3 | 17 | 4 | 8 | 0 |
| K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | K14 |
| 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 |
| 3 | 18 | 16 | 11 | 24 | 22 | 4 | 21 | 21 | 6 | 2 | 18 | 7 | 13 |
| **D** | **S** | **Q** | **L** | **Y** | **W** | **E** | **V** | **V** | **G** | **C** | **S** | **H** | **N** |

Criptarea:

E(x)≡(Im(x)+Im(cheii)) mod n ≡ y

In cazul nostru n=26

E(C)≡(2+1) mod 26 ≡ 3 (D)

Decriptarea:

D(y)≡(Im(y)-Im(cheii)) mod n ≡ x

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **D** | **S** | **Q** | **L** | **Y** | **W** | **E** | **V** | **V** | **G** | **C** | **S** | **H** | **N** |
| 3 | 18 | 16 | 11 | 24 | 22 | 4 | 21 | 21 | 6 | 2 | 18 | 7 | 13 |
| K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | K14 |
| 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 |
| 2 | 17 | 14 | 8 | 19 | 14 | 17 | 0 | 13 | 3 | 17 | 4 | 8 | 0 |
| **C** | **R** | **O** | **I** | **T** | **O** | **R** | **A** | **N** | **D** | **R** | **E** | **I** | **A** |

D(D)≡(3-1) mod 26 ≡ 2 (C)

D(E)≡(4-13) mod 26 ≡ (-9+26) ≡ 17 (R)

1. Sisteme de criptare cu chei fluide asincrone (auto-sincrone)

Vedeți partea teoretică

Text clar: **CRISTIAN**, cheia inițială, k1=7

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| C | R | I | S | T | I | A | N |
| 2 | 17 | 8 | 18 | 19 | 8 | 0 | 13 |
| K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 |
| 7 | 9 | 0 | 8 | 0 | 19 | 1 | 1 |
| 9 | 0 | 8 | 0 | 19 | 1 | 1 | 14 |
| J | A | I | A | T | B | B | O |

Criptarea:

E(x)≡(Im(x)+Im(cheii precedente)) mod n ≡ y

E(C)=(2+7) mod 26=9 (J)

E(R)=(17+9) mod 26=0 (A)

E(I)=(8+0) mod 26=8 (I)

E(S)=(18+8) mod 26=0 (A)

Text criptat:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| J | A | I | A | T | B | B | O |
| 9 | 0 | 8 | 0 | 19 | 1 | 1 | 14 |

D(Y)≡(Im(Y)-Im(cheii precedente)) mod n ≡ X

Decriptarea: CHEIA INITIALA

D(J)=(9-7) mod 26=2 (C)

D(A)=(0-9) mod 26= (-9+26) =17 (R)

D(I)=(8-0) mod 26=8 (I)

D(A)=(0-8) mod 26=(-8+26)=18 mod 26 = 18 (S)

D(T)=(19-0) mod 26=19 (T)

D(B)=(1-19) mod 26=8 (I)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| J | A | I | A | T | B | B | O |
| 9 | 0 | 8 | 0 | 19 | 1 | 1 | 14 |
| K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 |
| 7 | 9 | 0 | 8 | 0 | 19 | 1 | 1 |
| 2 | 17 | 8 | 18 | 19 | 8 | 0 | 13 |
| C | R | I | S | T | I | A | N |