

$$\begin{array}{r} 26 \\ 3 \\ \hline 78 \end{array}$$

$$\begin{array}{r} 72 \quad 26 \\ \hline 20 \end{array}$$

$$\begin{array}{r} 12 \\ 6 \\ \hline 72 \end{array}$$

$$\begin{array}{r} 12 \\ 25 \\ 60 \\ 24 \\ \hline 300 \end{array}$$

$$\begin{array}{r} 300 \quad 26 \\ \hline 286 \quad 14 \end{array}$$

$$\begin{array}{r} 260 \quad 12 \\ 11 \\ 260 \\ \hline 2860 \quad 260 \end{array}$$

Lista 03.

01. Obtenha a Cifra de Hill da mensagem AMOR para a matriz codificadora $K = \begin{pmatrix} 3 & 1 \\ 25 & 6 \end{pmatrix}$ em módulo 26. Encontra K^{-1} e decifre a mensagem.

$$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K) \quad \rightarrow E = (OR) \cdot \begin{pmatrix} 3 & 1 \\ 25 & 6 \end{pmatrix}$$

$$\det(K) = 3 \cdot 6 - 25 \cdot 1 = -7 + 26 = 19$$

Calcular $19^{-1} \bmod 26$

$$\text{MDC}(26, 19) \Rightarrow \begin{array}{c|cc|cc|c} 26 & 19 & 7 & 5 & 2 & \\ \hline 7 & 5 & 2 & 1 & & \end{array}$$

$$1 = 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7$$

$$1 = 3 \cdot 19 - 3 \cdot 2 \cdot 7 - 2 \cdot 7$$

$$1 = 3 \cdot 19 - 6 \cdot 7 - 2 \cdot 7$$

$$1 = 3 \cdot 19 - 8 \cdot 7$$

$$1^{\circ}: 26 = 1 \cdot 19 + 7 \quad \rightarrow 1 = 5 - 2 \cdot 2$$

$$2^{\circ}: 19 = 2 \cdot 7 + 5 \quad \rightarrow 1 = 5 - 2 \cdot (7 - 1 \cdot 5)$$

$$3^{\circ}: 7 = 1 \cdot 5 + 2 \quad \rightarrow 1 = 5 - 2 \cdot 7 + 2 \cdot 5$$

$$4^{\circ}: 5 = 2 \cdot 2 + 1 \quad \rightarrow 1 = 3 \cdot 5 - 2 \cdot 7$$

$$1 = 3 \cdot 19 - 8 \cdot (26 - 1 \cdot 19)$$

$$1 = 3 \cdot 19 - 8 \cdot 26 + 8 \cdot 19$$

$$1 = 11 \cdot 19 - 8 \cdot 26$$

$$19^{-1} \bmod 26 = 11 \quad \leftarrow \det(K)^{-1}$$

$$\text{adj}(K) = \text{cof}(K)^t$$

$$\bar{K} = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}$$

$$\bar{K}_{ij} = (-1)^{i+j} \cdot \det(K^{ij})$$

$$E \rightarrow (AM) = 0 \rightarrow 12, \begin{pmatrix} 3 & 1 \\ 25 & 6 \end{pmatrix}$$

$$\bar{K}_{11} = (-1)^2 \cdot \det(6) = 6 \quad \bmod$$

$$\bar{K}_{12} = (-1)^3 \cdot \det(25) = -25 + 26 = 1$$

$$\bar{K}_{21} = (-1)^3 \cdot \det(1) = -1 + 26 = 25$$

$$\bar{K}_{22} = (-1)^4 \cdot \det(3) = 1$$

$$0 \rightarrow 3 + 12 \cdot 25 \quad 0 \rightarrow 1 + 12 \cdot 6$$

$$14 \rightarrow (0) \quad 20 \rightarrow (1)$$

$$(-1) \rightarrow (0) R = 14 \rightarrow 12, \begin{pmatrix} 3 & 1 \\ 25 & 6 \end{pmatrix}$$

$$14 \rightarrow 3 + 17 \cdot 25 \quad 14 \rightarrow 1 + 17 \cdot 6$$

$$6467 \rightarrow (Z) \quad 616 \rightarrow (M)$$

$$5 \rightarrow 25 \quad 5 \rightarrow 12$$

$$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K)$$

$$K^{-1} = 11 \cdot \begin{pmatrix} 6 & 25 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 66 & 275 \\ 11 & 44 \end{pmatrix} \rightarrow \text{em módulo } 26 = \begin{pmatrix} 14 & 15 \\ 11 & 18 \end{pmatrix}$$

E = OUZM

02. $K = \begin{pmatrix} 6 & 24 & 1 & 13 \\ 13 & 16 & 10 & 20 \\ 20 & 17 & 15 & 19 \\ 9 & 3 & 8 & 7 \end{pmatrix}$ em módulo 26. texto claro $\rho = V_i / LA$

$$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K)$$

$\det(K) =$ Vamos usar Laplace

$$\hookrightarrow 1^{\text{a}} \text{ linha} \Rightarrow [6 \cdot C_{11} + 24 \cdot C_{12} + 1 \cdot C_{13} + 13 \cdot C_{14}]$$

$$C_{11} = (-1)^{1+1} \cdot \begin{vmatrix} 16 & 10 & 30 & 16 & 10 & 900 & 2432 & 1190 \end{vmatrix} = 4522$$

$$17 \quad 15 \quad 19 \quad 17 \quad 15$$

$$3 \quad 8 \quad 7 \quad 3 \quad 8$$

$$1680 \quad 570 \quad 2720 = 4970 \quad C_{11} = 448$$

$$\text{MOD } 26 = 16$$

$$C_{12} = (-1)^{1+2} \cdot \begin{vmatrix} 2700 & 1976 & 1400 & 6076 \\ 13 & 10 & 20 & 13 \cdot 10 \\ 20 & 15 & 19 & 20 \cdot 15 \\ 9 & 8 & 7 & 9 \cdot 8 \end{vmatrix} = -1 \cdot 199 = -199$$

$$C_{12} = -199$$

$$\text{MOD } 26 = 9$$

$$C_{13} = (-1)^{1+3} \cdot \begin{vmatrix} 1365 & 1710 & 3200 & 6275 \\ 13 & 16 & 20 & 13 \cdot 16 \\ 20 & 17 & 19 & 20 \cdot 17 \\ 9 & 3 & 7 & 9 \cdot 3 \end{vmatrix} = 5483 - 6041 = -558$$

$$C_{13} = -558$$

$$C_{14} = (-1)^{1+4} \cdot \begin{vmatrix} 1547 & 2736 & 1200 & 5483 \\ 1530 & 585 & 2860 & 4675 \\ 13 & 16 & 10 & 13 \cdot 16 \\ 20 & 17 & 15 & 20 \cdot 17 \end{vmatrix} = 4528 - 4675 = -147$$

$$-1 \cdot -147 = 147$$

$$C_{14} = 147$$

$$1^{\text{a}} \text{ linha} = 6 \cdot 448 + 24 \cdot (-199) + 1 \cdot (-558) + 13 \cdot 147 = -735 \quad \text{MOD } 26 = 17$$

$$-735 \text{ mod } 26 = 19$$

$\det(K)^{-1} \Rightarrow 19^{-1} \text{ mod } 26 \rightarrow$ já calculado no anterior; $\det(K)^{-1} = 11$.

$$\text{adj}(K) = \text{Cof}(K)^t$$

$$\bar{K} = \begin{pmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{pmatrix} \quad \bar{K}_{ij} = (-1)^{i+j} \cdot \det(K^*)$$

Cofatores da primeira linha já calculados.

$$K_{21} = (-1)^{2+1} \cdot \begin{vmatrix} 585 & 3678 & 119 & 4352 \\ 27 & 1 & 13 & 24 \\ 17 & 15 & 19 & 17 \\ 3 & 8 & 7 & 3 \end{vmatrix} \quad 4345 - 4352 = -7$$

$$-1 \cdot (-7) = 7$$

$$2520 \cdot 57 - 1768 = 4345 \quad \underline{K_{21} = 7}$$

$$K_{22} = (-1)^{2+2} \cdot \begin{vmatrix} 1255 & 816 & 140 & 2711 \\ 6 & 1 & 13 & 6 \\ 20 & 15 & 17 & 20 \\ 9 & 8 & 7 & 9 \end{vmatrix} \quad 2863 - 2711 = 152$$

$$630 \cdot 153 - 2080 = 2863 \quad \underline{K_{22} = 152}$$

Mod = 22

$$K_{23} = (-1)^{2+3} \cdot \begin{vmatrix} 1989 & 342 & 3360 & -5691 \\ 6 & 24 & 13 & 6 \\ 20 & 17 & 19 & 20 \\ 9 & 3 & 7 & 9 \end{vmatrix} \quad -1 \cdot 5598 - 5691 = 93$$

$$214 \cdot 4104 - 780 \cdot 5598 \quad \underline{K_{23} = 93}$$

Mod = 15

$$K_{24} = (-1)^{2+4} \cdot \begin{vmatrix} 153 & 270 & 3840 & 4263 \\ 6 & 24 & 1 & 6 \\ 20 & 17 & 15 & 20 \\ 9 & 3 & 8 & 9 \end{vmatrix} \quad 49 \cdot 14116 - 4263 = -147$$

 $K_{24} = -147$

Mod = 42/9

$$K_{31} = (-1)^{3+1} \cdot \begin{vmatrix} 816 & 3240 & 60 & 4116 \\ 24 & 1 & 13 & 24 \\ 16 & 10 & 20 & 16 \\ 3 & 8 & 7 & 3 \end{vmatrix} \quad 816 \cdot 3240 - 60 \cdot 4116 = 4342$$

$$-1 \cdot 4342 = -4342 \quad \rightarrow +1 \cdot -938$$

$$1680 \cdot 60 - 1664 \cdot 3404 \quad \underline{K_{31} = -938}$$

Mod = 24

$$\bar{K}_{32} = (-1)^{3+2} \begin{vmatrix} 6 & 1 & 13 & 6 & 1 \\ 13 & 10 & 20 & 13 & 10 \\ 9 & 8 & 7 & 9 & 8 \end{vmatrix} \quad 1170 \cdot 960 \cdot 99 = 2221$$

$$-1 \cdot -269 \quad \bar{K}_{32} = 269 \quad \text{mod} = 9$$

$$\bar{K}_{33} = (-1)^{3+3} \begin{vmatrix} 6 & 24 & 13 & 6 & 24 \\ 13 & 16 & 20 & 13 & 16 \\ 9 & 3 & 7 & 9 & 3 \end{vmatrix} \quad 1872 \cdot 360 \cdot 2184 = 4416$$

$$-5799 - 4416 = 1083 \quad \bar{K}_{33} = 1083 \quad \text{mod} = 17$$

$$\bar{K}_{34} = (-1)^{3+4} \begin{vmatrix} 6 & 24 & 1 & 6 & 24 \\ 13 & 16 & 10 & 13 & 16 \\ 9 & 3 & 8 & 9 & 3 \end{vmatrix} \quad 144 \cdot 180 \cdot 2446 = 2820$$

$$-1 \cdot 147 \quad \bar{K}_{34} = -147 \quad -17 + 26 \quad \text{mod} = 9$$

$$\bar{K}_{41} = (-1)^{4+1} \begin{vmatrix} 24 & 1 & 13 & 24 & 1 \\ 16 & 10 & 20 & 16 & 10 \\ 17 & 15 & 19 & 17 & 15 \end{vmatrix} \quad 2210 \cdot 7200 \cdot 304 = 9714$$

$$-1 \cdot -1694 \quad \bar{K}_{41} = 1694 \quad \text{mod} = 9$$

$$\bar{K}_{42} = (-1)^{4+2} \begin{vmatrix} 6 & 1 & 13 & 6 & 1 \\ 13 & 10 & 20 & 13 & 10 \\ 20 & 15 & 19 & 20 & 15 \end{vmatrix} \quad 4560 \cdot 340 \cdot 3120 = 8020$$

$$4075 - 4647 = -572 \quad \bar{K}_{42} = -572 \quad \text{mod} = 0$$

$$\bar{K}_{43} = (-1)^{4+3} \begin{vmatrix} 6 & 24 & 13 & 6 & 24 \\ 13 & 16 & 20 & 13 & 16 \\ 20 & 17 & 19 & 20 & 17 \end{vmatrix} \quad 4160 \cdot 2040 \cdot 5928 = 12128$$

$$-1 \cdot (14897 - 12128) = 2169 \quad \bar{K}_{43} = -2169 \quad \text{mod} = 15$$

$$\bar{K}_{44} = (-1)^{4+4} \begin{vmatrix} 6 & 24 & 1 & 6 & 24 \\ 13 & 16 & 10 & 13 & 16 \\ 20 & 17 & 15 & 20 & 17 \end{vmatrix} \quad 320 \cdot 9020 \cdot 4680 = 6020$$

$$6461 - 6020 = 441 \quad \bar{K}_{44} = 441 \quad 441 \quad \text{mod} = 25$$

$$1440 \cdot 4800 \cdot 221 = 6461 \quad \text{mod} = 25$$

MOD 26

$$K = \begin{pmatrix} 6 & 9 & 14 & 17 \\ 7 & 22 & 15 & 9 \\ 24 & 9 & 17 & 9 \\ 4 & 0 & 15 & 25 \end{pmatrix} \xrightarrow{\text{adj}(K)} \begin{pmatrix} 6 & 7 & 24 & 4 \\ 9 & 22 & 9 & 0 \\ 14 & 15 & 17 & 15 \\ 17 & 9 & 9 & 25 \end{pmatrix}$$

adj(K)

$$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K)$$

$$\rightarrow K^{-1} = 11 \cdot \begin{pmatrix} 6 & 7 & 24 & 4 \\ 9 & 22 & 9 & 0 \\ 14 & 15 & 17 & 15 \\ 17 & 9 & 9 & 25 \end{pmatrix} = \begin{pmatrix} 66 & 77 & 264 & 44 \\ 99 & 242 & 99 & 0 \\ 154 & 165 & 187 & 165 \\ 187 & 99 & 99 & 275 \end{pmatrix}$$

$$\text{um mod } 26 = \begin{pmatrix} 14 & 25 & 9 & 18 \\ 21 & 8 & 21 & 0 \\ 24 & 9 & 5 & 9 \\ 5 & 21 & 21 & 15 \end{pmatrix} \cdot K^{-1}$$

um mod 26

$$\text{Encryption} \rightarrow \text{VILA} \Rightarrow (21 \ 8 \ 11 \ 0) \cdot K = [8 \ 13 \ 6 \ 18]$$

$$E = \text{INGENIERIE} \Rightarrow (21 \ 8 \ 13 \ 6 \ 18) \cdot K^{-1} = [21 \ 8 \ 11 \ 0]$$

$$\text{Decryption} \rightarrow \text{INGENIERIE} \Rightarrow (8 \ 13 \ 6 \ 18) \cdot K^{-1} = [21 \ 8 \ 11 \ 0]$$

G1

G2

G3

G4

G5

G6

G7

G8

G9

G10

G11

G12

G13

G14

G15

G16

G17

G18

G19

G20

G21

G22

G23

G24

G25

G26

G27

G28

G29

G30

G31

G32

G33

G34

G35

G36

G37

G38

G39

G40

G41

G42

G43

G44

G45

G46

G47

G48

G49

G50

G51

G52

G53

G54

G55

G56

G57

G58

G59

G60

G61

G62

G63

G64

G65

G66

G67

G68

G69

G70

G71

G72

G73

G74

G75

G76

G77

G78

G79

G80

G81

G82

G83

G84

G85

G86

G87

G88

G89

G90

G91

G92

G93

G94

G95

G96

G97

G98

G99

G100

G101

G102

G103

G104

G105

G106

G107

G108

G109

G110

G111

G112

G113

G114

G115

G116

G117

G118

G119

G120

G121

G122

G123

G124

G125

G126

G127

G128

G129

G130

G131

G132

G133

G134

G135

G136

G137

G138

G139

G140

G141

G142

G143

G144

G145

G146

G147

G148

G149

G150

G151

G152

G153

G154

G155

G156

G157

G158

G159

G160

G161

G162

G163

G164

G165

G166

G167

G168

G169

G170

G171

G172

G173

G174

G175

G176

G177

G178

G179

G180

G181

G182

G183

G184

G185

G186

G187

G188

G189

G190

G191

G192

G193

G194

G195

G196

G197

G198

G199

G200

G201

G202

G203

G204

G205

G206

G207

G208

G209

G210

G211

G212

G213

G214

G215

G216

G217

G218

G219

G220

G221

G222

G223

G224

G225

G226

G227

G228

G229

G230

G231

G232

G233

G234

G235

G236

G237

G238

G239

G240

G241

G242

G243

G244

G245

G246

G247

G248

G249

G250

G251

G252

G253

G254

G255

G256

G257

G258

G259

G260

G261

G262

G263

G264

<p

03. Determinar a K^{-1} em \mathbb{Z}_5 da matriz: $A = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix}$

$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K)$

$\det(K)$ por Laplace - 3^ª linha

$$K_{31} = (-1)^{3+1} \cdot \begin{vmatrix} 1 & 2 \\ 1 & 2 \end{vmatrix} = 2 - 2 = 0$$

$$K_{32} = (-1)^{3+2} \cdot \begin{vmatrix} 3 & 2 \\ 1 & 2 \end{vmatrix} = 6 - 2 = 4 \rightarrow 1 = -4 \pmod{5} = 1$$

$$K_{33} = (-1)^{3+3} \cdot \begin{vmatrix} 3 & 1 \\ 1 & 1 \end{vmatrix} = 3 - 1 = 2$$

$$\det(K) = 0 \cdot 0 + 1 \cdot (-4) + 3 \cdot (2) = -4 + 6 = 2$$

$$2^{-1} \pmod{5} = 3$$

$\text{adj}(K) = \text{cof}(K)^t$

$\text{cof}(K) =$ já temos a última linha

$$K_{11} = (-1)^{1+1} \cdot \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = 3 - 2 = 1 \quad K_{11} = 1$$

$$K_{12} = (-1)^{1+2} \cdot \begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix} = 3 - 0 = 3 \rightarrow K_{12} = -3 \pmod{5} = 2$$

$$K_{13} = (-1)^{1+3} \cdot \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1 - 0 = 1 \rightarrow K_{13} = 1$$

$$K_{21} = (-1)^{2+1} \cdot \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = 1 - 2 = -1 \rightarrow K_{21} = -1 \pmod{5} = 4$$

$$K_{22} = (-1)^{2+2} \cdot \begin{vmatrix} 3 & 2 \\ 0 & 3 \end{vmatrix} = 9 - 0 = 9 \rightarrow K_{22} = 9 \pmod{5} = 4$$

$$K_{23} = (-1)^{2+3} \cdot \begin{vmatrix} 3 & 1 \\ 0 & 1 \end{vmatrix} = 3 - 0 = 3 \rightarrow K_{23} = -3 \pmod{5} = 2$$

$$\text{cof}(K) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 1 \\ 4 & 4 & 2 \end{pmatrix} \Rightarrow \text{cof}(K)^t = \begin{pmatrix} 0 & 1 & 4 \\ 1 & 2 & 4 \\ 2 & 1 & 2 \end{pmatrix}$$

$$K^{-1} = 3 \cdot \text{adj}(K) = \begin{bmatrix} 0 & 3 & 12 \\ 3 & 6 & 12 \\ 6 & 3 & 6 \end{bmatrix} \rightarrow \text{modulo } 5 = \begin{bmatrix} 0 & 3 & 2 \\ 3 & 1 & 2 \\ 1 & 3 & 1 \end{bmatrix}$$

4) $\rho = \text{FLAMENGO}$ $K = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ um mód 26

$$K^{-1} = \det(K)^{-1} \cdot \text{adj}(K)$$

$\det(K)$ com Laplace

↳ Usar 2ª linha

$$\det = 1 \cdot K_{21} + 0 \cdot K_{22} + 0 \cdot K_{23} + 0 \cdot K_{24}$$

$$\bar{K}_{21} = (-1)^{2+1} \cdot \begin{vmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 2 & 3 & 4 & 2 \\ 4 & 0 & 3 & 7 \end{vmatrix} \quad 7 - 2 = 5 \Rightarrow 5 - 1 = -5$$

$$\bar{K}_{21} = -5$$

$$\det(K)^{-1} = -5^{-1} \text{ mód } 26 = 5$$

$$\text{adj}(K) = \text{cof}(K)^t$$

$$\begin{pmatrix} 0 & \bar{K}_{22} & 0 & \bar{K}_{13} \\ \bar{K}_{21} & 0 & 0 & 0 \\ 0 & \bar{K}_{32} & \bar{K}_{33} & 0 \\ \bar{K}_{41} & \bar{K}_{42} & \bar{K}_{43} & \bar{K}_{44} \end{pmatrix} \bar{K}_{12} = (-1)^{2+2} \cdot \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 3 & 4 & 1 & 3 \\ 4 & 0 & 0 & 1 & 0 \end{vmatrix} = 0$$

$$\bar{K}_{12} = -4 \text{ mód } 26 = 22$$

$$\bar{K}_{13} = (-1)^5 \cdot \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 3 & 1 & 2 \\ 3 & 0 & 0 & 1 & 0 \end{vmatrix} = 3 - 2 = 1 - 1 = 0 \text{ s/ jiz } \bar{K}_{21} = 21$$

$$\bar{K}_{13} = -1 \text{ mód } 26 = 25$$

$$\bar{K}_{32} = (-1)^5 \cdot \begin{vmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 3 & 4 & 1 & 3 & 0 \\ 0 & 0 & 3 & 3 & 0 & 3 \end{vmatrix} = 3 - 0 = 3 - 1 \rightarrow \bar{K}_{32} = -3$$

$$\text{mód } 26 = 23$$

$$\bar{K}_{33} = (-1)^6 \cdot \begin{vmatrix} 0 & 1 & 1 & 0 & 1 & 4 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 4 & 1 & 2 & 0 \\ 0 & 0 & 2 & 0 & 0 & 2 \end{vmatrix} = 2 - 4 = -2 \text{ mód } 26 = \bar{K}_{33} = 24$$

$$K_{44} = -1^5 \cdot \begin{vmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{vmatrix} \quad K_{14} = (0)$$

$$\bar{K}_{42} = -1^6 \cdot \begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{vmatrix} \quad 1 - 0 = 1 \quad \bar{K}_{42} = (1)$$

$$\bar{K}_{43} = -1^7 \cdot \begin{vmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{vmatrix} \quad 1 - 0 = 1 \cdot -1 = -1 \bmod 26 = 25 \quad \bar{K}_{43} = (25)$$

$$\bar{K}_{44} = -1^8 \cdot \begin{vmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{vmatrix} \quad 0 - 1 = -1 + 26 = 25 \quad \bar{K}_{44} = (25)$$

$$\text{cof}(K) = \begin{pmatrix} 0 & 22 & 0 & 25 \\ 21 & 0 & 0 & 0 \\ 0 & 23 & 24 & 0 \\ 0 & 1 & 25 & 25 \end{pmatrix} = \text{cof}(K)^t \cdot \begin{pmatrix} 0 & 21 & 0 & 0 \\ 22 & 0 & 23 & 1 \\ 0 & 0 & 24 & 25 \\ 25 & 0 & 0 & 25 \end{pmatrix} = \text{adj}(K)$$

$$K^{-1} = 5 \cdot \text{adj}(K) \cdot \text{fim m módulo } 26 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 6 & 0 & 14 & 5 \\ 0 & 0 & 16 & 21 \\ 21 & 0 & 0 & 21 \end{pmatrix}$$

05. Obtenha a cifra afim da mensagem ENCRYPTION para a função codificadora $E_K(x) = 17x + 7 \pmod{26}$. Encontre a função inversa e decifre a mensagem.

$$E: 4 \quad N: 13 \quad C: 2 \quad R: 17 \quad Y: 24 \quad P: 15 \quad T: 19 \quad I: 8$$

$$O: 14 \quad N: 13$$

$$E_K(x) = 17x + 7 \pmod{26}$$

$$C \rightarrow 17 \cdot 4 + 7 \pmod{26} = 23 \rightarrow X$$

$$N \rightarrow 17 \cdot 13 + 7 \pmod{26} = 20 \rightarrow U$$

$$C \rightarrow 17 \cdot 2 + 7 \pmod{26} = 15 \rightarrow P$$

$$R \rightarrow 17 \cdot 17 + 7 \pmod{26} = 10 \rightarrow K$$

$$Y \rightarrow 17 \cdot 24 + 7 \pmod{26} = 25 \rightarrow Z$$

$$P \rightarrow 17 \cdot 15 + 7 \pmod{26} = 2 \rightarrow U$$

$$T \rightarrow 17 \cdot 19 + 7 \pmod{26} = 18 \rightarrow S$$

$$I \rightarrow 17 \cdot 8 + 7 \pmod{26} = 13 \rightarrow N$$

$$O \rightarrow 17 \cdot 14 + 7 \pmod{26} = 11 \rightarrow L$$

$$N \rightarrow 17 \cdot 13 + 7 \pmod{26} = 20 \rightarrow V$$

$$d_K(y) = 23(y - 7) \pmod{26} \Rightarrow d_K(y) = 23y - 5 \pmod{26}$$

$$X \rightarrow 23 \cdot 23 - 5 \pmod{26} = 4 \rightarrow G$$

$$U \rightarrow 23 \cdot 20 - 5 \pmod{26} = 13 \rightarrow N$$

$$P \rightarrow 23 \cdot 15 - 5 \pmod{26} = 2 \rightarrow C$$

$$K \rightarrow 23 \cdot 10 - 5 \pmod{26} = 17 \rightarrow R$$

$$Z \rightarrow 23 \cdot 25 - 5 \pmod{26} = 24 \rightarrow Y$$

$$V \rightarrow 23 \cdot 2 - 5 \pmod{26} = 15 \rightarrow P$$

$$S \rightarrow 23 \cdot 18 - 5 \pmod{26} = 19 \rightarrow T$$

$$N \rightarrow 23 \cdot 13 - 5 \pmod{26} = 8 \rightarrow I$$

$$L \rightarrow 23 \cdot 11 - 5 \pmod{26} = 14 \rightarrow O$$

$$U \rightarrow 23 \cdot 20 - 5 \pmod{26} = 13 \rightarrow N$$

2 2 2 2 2 2

letra + frequente
em inglês

$$8 \cdot 06 - E \rightarrow B \rightarrow T \rightarrow U$$

CIFRA AFIM:

$$\begin{aligned} B &= (aE + b) \bmod 26 \\ U &= (aT + b) \bmod 26 \\ 1 &= (a \cdot 4 + b) \bmod 26 \\ 20 &= (a \cdot 19 + b) \bmod 26 \end{aligned}$$

$$\begin{cases} 1 = 4a + b \bmod 26 \\ 20 = 19a + b \bmod 26 \end{cases}$$

$$(20 - 1) = (19a - 4a) \bmod 26$$

$$19 = 15a \bmod 26$$

$$15a = 19 \bmod 26$$

$$15^{-1} \bmod 26 = 7$$

$$a = 19 \cdot 7 \bmod 26$$

$$a = 133 \bmod 26$$

$$a = 3 \bmod 26$$

$$1 = 4 \cdot 3 + b \bmod 26$$

$$1 = 12 + b \bmod 26$$

$$b = -11 + 26 = 15 \bmod 26$$

Decifrar o texto

↳ função inversa da cifra Afim

$$P = a^{-1} (C - b) \bmod 26$$

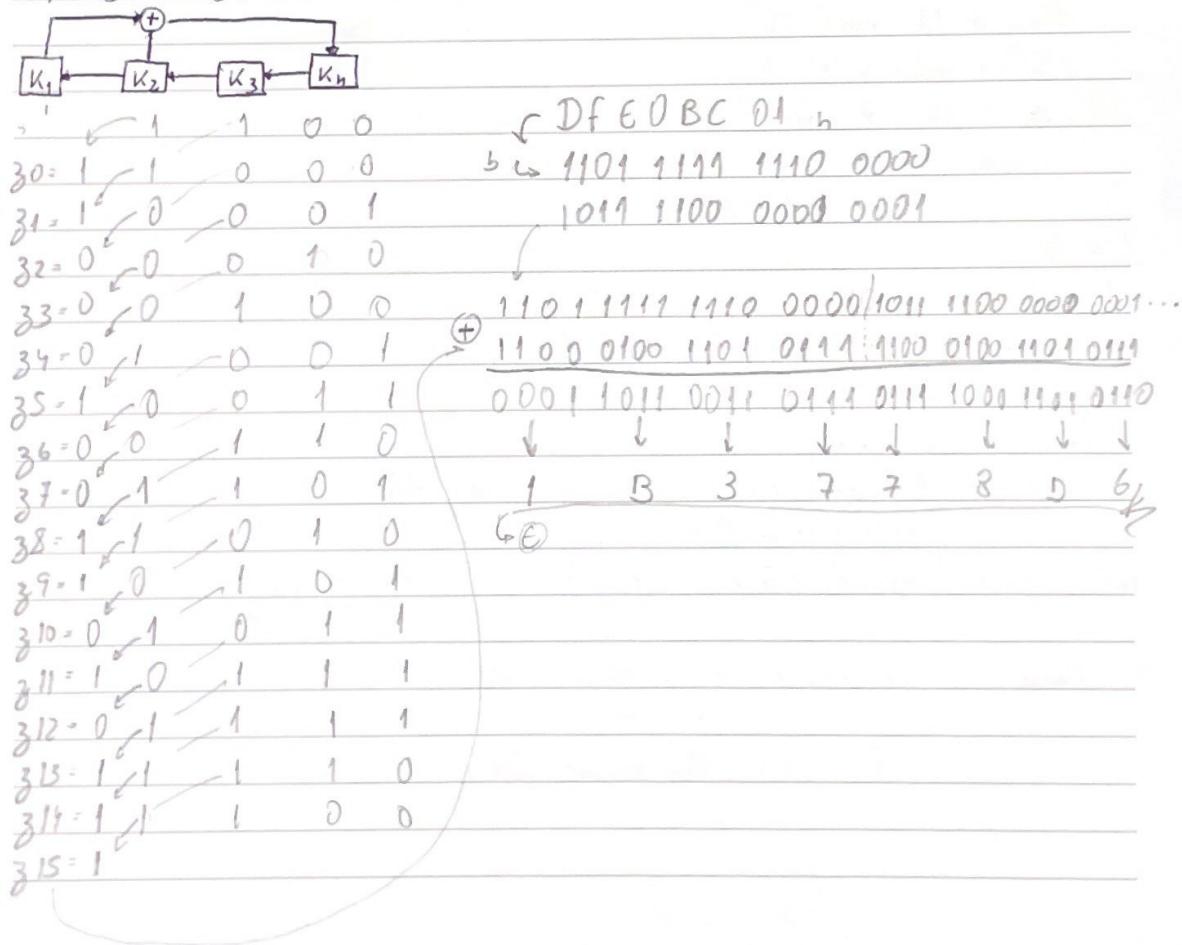
$$a \cdot 3 \rightarrow 3^{-1} \bmod 26 = 9 \quad \text{e} \quad P = 9(C - 15) \bmod 26$$

Para decifrar esse texto aplicamos a fórmula

$$P = 9(C - 15) \bmod 26$$

07. Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo? As cifras de bloco criptografam dados em blocos fixos, enquanto cifras de fluxo operam bit a bit ou byte a byte. Exemplo, de blocos criptografa "Hello" como um bloco intiero, e a de fluxo cifra cada letra individualmente.

08. Usando Linear Feedback Shift Register e como vetor de inicialização: $(1, 1, 0, 0)$, após obter a chave cifre a mensagem $m = DFE0BC01(n)$ com $C(x_i) = x_i + k_i \bmod 2$



$$\begin{array}{r}
 5 \ 2^4 \ 2^3 \ 2^2 \ 2^1 \ 2^0 \\
 32 \ 16 \ 8 \ 4 \ 2 \ 1 \\
 \hline
 1 \ 0 \ 0 \ 0 \ 0 \ 1 \rightarrow 16
 \end{array}$$

09. Obter a chave fechada para a mensagem $M = \text{UNIVERSIDADE}$. Sua chave: $K = 16$ (semente). Cifrar e Decifrar com $G(m_i) = m_i + K \pmod{26}$ e $D(y_i) = y_i - K \pmod{26}$
 $K = 16 \rightarrow 10000$

$\text{UNIVERSIDADE} \Rightarrow 20 \ 13 \ 8 \ 21 \ 4 \ 17 \ 18 \ 8 \ 3 \ 0 \ 3 \ 4$

$$E(m_i) = m_i + K \pmod{26}$$

$$U = (20 + 16) \pmod{26} = 10 \rightarrow K$$

$$N = (13 + 16) \pmod{26} = 23 \rightarrow X$$

$$I = (8 + 16) \pmod{26} = 5 \rightarrow F$$

$$V = (21 + 16) \pmod{26} = 0 \rightarrow A$$

$$E = (4 + 16) \pmod{26} = 4 \rightarrow G$$

$$R = (17 + 16) \pmod{26} = 21 \rightarrow V$$

$$S = (18 + 16) \pmod{26} = 13 \rightarrow N$$

$$I = (8 + 16) \pmod{26} = 21 \rightarrow V$$

$$D = (3 + 16) \pmod{26} = 24 \rightarrow Y$$

$$A = (0 + 16) \pmod{26} = 24 \rightarrow Y$$

$$D = (3 + 16) \pmod{26} = 1 \rightarrow B$$

$$E = (4 + 16) \pmod{26} = 5 \rightarrow F$$

Decifrar = $D(y_i) = y_i - K$

$$K = (10 - 16)$$

$$X = (23 - 16) \pmod{26} = 20 \rightarrow U$$

$$F = (5 - 16) \pmod{26} = 13 \rightarrow N$$

$$A = (0 - 16) \pmod{26} = 8 \rightarrow I$$

$$G = (4 - 16) \pmod{26} = 21 \rightarrow V$$

$$V = (21 - 16) \pmod{26} = 4 \rightarrow G$$

$$N = (13 - 16) \pmod{26} = 17 \rightarrow R$$

$$V = (21 - 16) \pmod{26} = 18 \rightarrow S$$

$$Y = (24 - 16) \pmod{26} = 8 \rightarrow I$$

$$Y = (24 - 16) \pmod{26} = 3 \rightarrow J$$

$$B = (1 - 16) \pmod{26} = 0 \rightarrow A$$

$$F = (5 - 16) \pmod{26} = 3 \rightarrow J$$

10. Diferença entre cifra polialfabética e monoalfabéticas.
mono \Rightarrow Usa apenas um alfabeto de substituição (ex: Cesar)
poli \Rightarrow Usa múltiplos alfabetos de substituição que variam ao longo do texto (ex: Vigenère)

11. Em uma cifra afim $E(x) = ax + b \text{ mod } 53$, determine quais valores de a não são permitidos.

Para a cifra ser válida, o valor de a deve ter um inverso modular em relação a 53.

$$\Leftrightarrow a \cdot a^{-1} \equiv 1 \text{ mod } 53$$

53 é primo, logo os números a que possuem inverso modular são todos os números inteiros entre 1 a 52 que são coprimos com 53. Como 53 é primo, qualquer número de 1 a 52 não é coprimo com 53

12. Um serviço secreto precisa enviar uma mensagem a um agente. A mensagem é codificada, usando uma chave que o agente escolhe conhece, e encrada por um portador. Como proteção extra, caso seja interceptado, o portador leva uma mensagem falsa também codificada e a mensagem verdadeira oculta em uma cápsula implantada sob a pele. O exemplo pode ser identificado como criptografia ou esteganografia? Explique.

Esse exemplo combina criptografia com esteganografia. (mensagem verdadeira oculta na cápsula sob a pele). A criptografia protege o conteúdo, enquanto a esteganografia oculta sua existência.

13. Usando cifra de Cesar e com deslocação de 11 posições:

"HPMTWGXPPLEXTOYTRSE"

$$H - 7 \rightarrow 7 - 11 = -4 + 26 = 22 \rightarrow W$$

$$P - 15 \rightarrow 15 - 11 = 4 \rightarrow E$$

$$M - 7 \rightarrow 7 - 11 = -4 + 26 = 22 \rightarrow W$$

$$T - 19 \rightarrow 19 - 11 = 8 \rightarrow I$$

$$W - 22 \rightarrow 22 - 11 = 11 \rightarrow L$$

$$W - 22 \rightarrow 22 - 11 = 11 \rightarrow L$$

$$X - 23 \rightarrow 23 - 11 = 12 \rightarrow M$$

$$P - 15 \rightarrow 15 - 11 = 4 \rightarrow E$$

$$D - 15 \rightarrow 15 - 11 = 4 \rightarrow E$$

$$G - 4 \rightarrow 4 - 11 = -7 + 26 = 19 \rightarrow T$$

$$L - 11 \rightarrow 11 - 11 = 0 \rightarrow A$$

$$E - 4 \rightarrow 4 - 11 = -7 + 26 = 19 \rightarrow T$$

$$X - 23 \rightarrow 23 - 11 = 12 \rightarrow M$$

$$T - 19 \rightarrow 19 - 11 = 8 \rightarrow I$$

$$O - 14 \rightarrow 14 - 11 = 3 \rightarrow D$$

$$Y - 24 \rightarrow 24 - 11 = 13 \rightarrow N$$

$$F - 19 \rightarrow 19 - 11 = 8 \rightarrow I$$

$$R - 17 \rightarrow 17 - 11 = 6 \rightarrow G$$

$$S - 18 \rightarrow 18 - 11 = 7 \rightarrow H$$

$$E - 4 \rightarrow 4 - 11 = -7 + 26 = 19 \rightarrow T$$

→ WE WILL GET AT MI ON EIGHT