Quadrat de Polibi - Far - Semaphore

Autor:
Data de publicació: 13-11-2021

Inventat cap al 150 aC per l'historiador Polibi, el quadrat de Polibi va ser utilitzat principalment pels nihilistes russos tancats a les presons tsaristes.

Es tracta d'un algorisme trivial, en què cada lletra de l'alfabet és reemplaçada per les coordenades de la seva posició en un quadrat. És un cas particular de transposició monoalfabètica, en el qual hi ha fragmentació (cada símbol del missatge original acaba dividit en més d'un símbol del missatge xifrat).

Aquest tipus de codi no resisteix una anàlisi de freqüències.

Inventat cap al 150 aC per l'historiador Polibi, el quadrat de Polibi va ser utilitzat principalment pels nihilistes russos tancats a les presons tsaristes.

Es tracta d'un algorisme trivial, en què cada lletra de l'alfabet és reemplaçada per les coordenades de la seva posició en un quadrat. És un cas particular de transposició monoalfabètica, en el qual hi ha fragmentació (cada símbol del missatge original acaba dividit en més d'un símbol del missatge xifrat).

Aquest tipus de codi no resisteix una anàlisi de freqüències.

Encriptació

Partim d'una matriu de 5x5 en què cada casella és una lletra de l'abecedari, i a la qual tenim indicat el nombre de cada fila i columna a mode de coordenades. En aquest cas hem posat la I i la J juntes per tal d'encabir l'abecedari de 26 lletres en una matriu de 25 caselles, tot i que una altra variant habutual ajunta la U i la V.

És possible estendre la matriu a 36 caselles per tal de poder-hi afegir també les xifres i alguns signes de puntuació.

12345

1
A
B
C
D
E

2
F

G
H
I/J
K

3
L
M
N
O
P

4
Q
R
S
T
U

5
V
W
X
Y
Z

Un cop tenim la matriu preparada, per codificar un text només hem de substituir cadascuna de les lletres per les seves coordenades: C esdevindrà 13, Y esdevindrà 54, etc.

Posant un exemple, si vull codificar "Moltes felicitats Clara", el missatge xifrat em quedaria:

Missatge normal: M O L T E S F E L I C I T A T S C L A R A
Missatge xifrat: 32 34 31 44 15 43 21 15 31 24 13 24 44 11 44 43 13 31 11 42 11

En aquest cas hem mantingut els nombres separats de dos en dos per facilitar-ne la lectura, però típicament s'escriurien tots seguits, dificultant el procés de deduir que dos números equivalen a una lletra.

Utilització de claus
Un sistema molt simple per poder compartir quadrats de Polibi entre emissor i receptor sense haver de recordar tota la matriu és generar-la a partir d'una paraula clau que és més fàcilment memoritzable. Per generar el quadrat de Polibi, es parteix de la paraula clau i es va omplint la matriu primer posant les lletres de la clau, sense repetir-les i, un cop acabades, completant la matriu amb les lletres de l'abecedari que falten, en ordre alfabètic.

Per exemple, si la paraula clau és “CRIPTOGAF” la matriu resultant seria:

12345

1
C
R
I/J

P
T

2
O
G
A
F
B

3
D
E
H
K
L

4
M
N
Q
S
U

5
V
W
X
Y
Z

Anècdota
Polibi havia imaginat una solució per transmetre els missatges amb torxes cremant. És una variant del codi morse.

Vegeu també

Xifratge clàssic
Història de la criptografia