1. ARITMÈTICA MODULAR

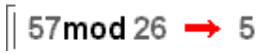
El significat matemàtic de l'expressió "(mod26)" al costat d'un nombre o una funció vol dir textualment: "si el nombre o resultat d'aplicar la fórmula sobrepassen el valor 25, cal reduir-lo a un valor comprès entre 0 i 25". Vegem com es pot reduir aquest valor. Per exemple, quant val 57(mod26)? Ens hem d'imaginar que estem a la taula del valor numèric situats damunt del valor 0 (que equival a la lletra A) i que ens comencem a desplaçar cap a la dreta de la taula, una casella cada vegada, fins un total de 57 vegades. Cada cop que arribeu al final de la taula i ja no quedin més caselles a la dreta, hem de tornar al principi damunt del valor 0 i continuar el procés. És com si la taula, en lloc de ser lineal, fos circular. S'ha de recorrer cíclicament tantes vegades com calgui fins a completar el nombre de desplaçaments indicats, 57 en aquest cas. Com que $26+26=52$, després de 52 desplaçaments haurem fet 2 recorreguts complets a la taula i tornarem a estar en el valor 0. Només caldrà fer 5 desplaçaments més per completar els 57, ja que $26+26+5=57$. Així, després de 57 desplaçaments estarem en la casella 5, que correspon a la lletra F. Per tant, $57(\text{mod}\,26)=5$.

La conclusió és: **el valor de** $k(\text{mod}\,n)$ **és igual a la resta que queda en dividir *k* entre *n*.** S'utilitza la divisió entre nombres enters que és fàcil de programar amb calculadores o ordinadors.

Estem molt acostumats a utilitzar el llenguatge modular en la nostra vida quotidiana. Per exemple, en qüestions horàries. Si són les 10 i ens diuen que hem de dinar d'aquí 5 hores, immediatament sabem que dinarem a les 3 de la tarda. En realitat hem fet la suma $10+5=15$ i després hem reduït el resultat a mòdul 12: $15(\text{mod}12)=3$. En la criptografia s'utilitza molt l'aritmètica modular.

Existeixen programes i calculadores que ja porten incorporades funcions per fer càlculs modulars, com la Wiris (calculadora proposada en la web www.edu365.cat). Vegem uns exemples:

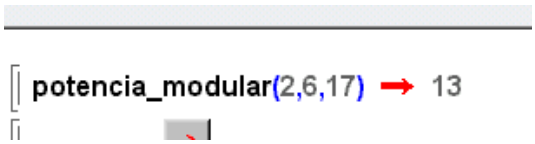
Quin és el residu de dividir 57 entre 26, *es llegeix 57 mòdul 26.* La Wiris ens dóna el resultat al moment.



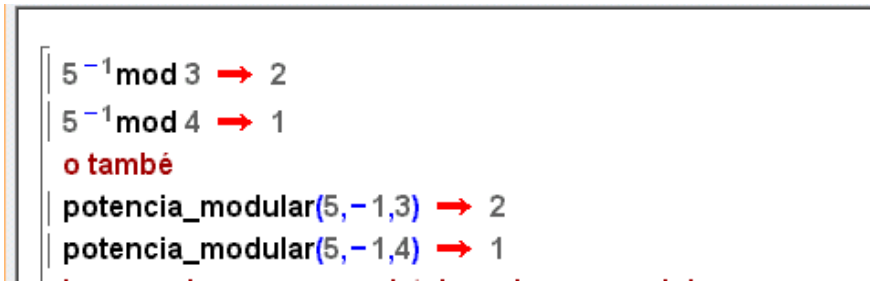
Aquest exemple sezill també es pot realitzar amb eines senzilles com el full de càlcul de l'Excel, la calculadora del sistema operatiu Windows i algunes calculadores científiques.

La Wiris també ens permet fer càlculs amb aritmètica modular més avançats com és el cas del càlcul de potències, que són la base del sistema criptogràfic RSA.

Quant val 2 elevat a 6 mòdul 17? És a dir, si elevem 2 a la sisena potència, quin residu tenim en dividir entre 17? Observació: $2^6 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 64$



També es pot operar amb inversos de l'aritmètica modular. Quin és l'invers de 5 mòdul 3? i el de 5 mòdul 4?



Aquestes dues operacions són més avançades i no les farem servir. Només les incloc per saber el llenguatge que utilitza la Wiris en el cas que es vulguin fer aquests càlculs.

2. ANÀLISI DE FREQÜÈNCIA

Per comoditat a l'hora d'explicar i per no perdre el fil, he inclòs les dades de l'anàlisi del text xifrat a l'annex ja que trobo que no són imprescindibles per entendre el mètode. No obstant, és una feina important que requereix molt de temps i esforç. Només per fer el recompte de les lletres i per ordenar-les en ordre decreixent segons els resultats vaig trigar una hora.

Recordem el text xifrat:

LYPUFHADLLUADLLOHLFUTEFEBLYTEIFGFOWLHFEHWJFHDOFXLT
OFTFSHLOBHLDOWXTPTYTOWLOEHFHLOLUKWOBLUYZHFOYGTDH
LFUKWOBLBLJWTFOFHYLYJEDFOEFULYSLHFBDOFWSWHEDOTEFES
LHLMLHPTHFHFIFFKJEWELYULYSWYYTJTUTEFEYBDOFBDUEUFYL
GFTHHLBDPETJULGWPFPTWBLKFUGFEADLYRFGTFBLSWYYFHLOKF
HMFFUFSHTKLHFWPFYTWADLLYSHLYLOELYBLKWKLOESLHPWKL
OÇFHYRFGTFRFZDEBLPWOXWHKFHFKJUWXLHEFBLUYLDWOPULB
LEHLJFUUFHFUEFUULHBLUYLKJFUFEZLYTGFSFYYFHULYETDLOEH
LPFHEWOYXDYELYTSFSLHYFSHLOLOTPWKLYXFJHTPFGLOLUYLOG
FYWYBLMTUSHWBDPELY

El recompte de les lletres del text xifrat vé donat en la següent taula que mostra el número de vegades que apareix cada lletra i el seu percentatge.

Lletres del text xifrat	Número de cops que apareix	Percentatge
L	67	14'41%
F	62	13'33%
H	41	8'81%
Y	37	7'96%
E	30	6'45%
O	29	6'24%
T	27	5'80%
U	27	5'80%
W	26	5'59%
B	18	3'87%

D	18	3’87%
K	14	3’01%
P	14	3’01%
S	14	3’01%
J	9	1’93%
G	8	1’73%
X	6	1’29%
A	4	0’86%
R	3	0’65%
Z	3	0’65%
I	2	0’43%
M	2	0’43%
Ç	1	0’22%
N	0	0
V	0	0
C	0	0
Q	0	0

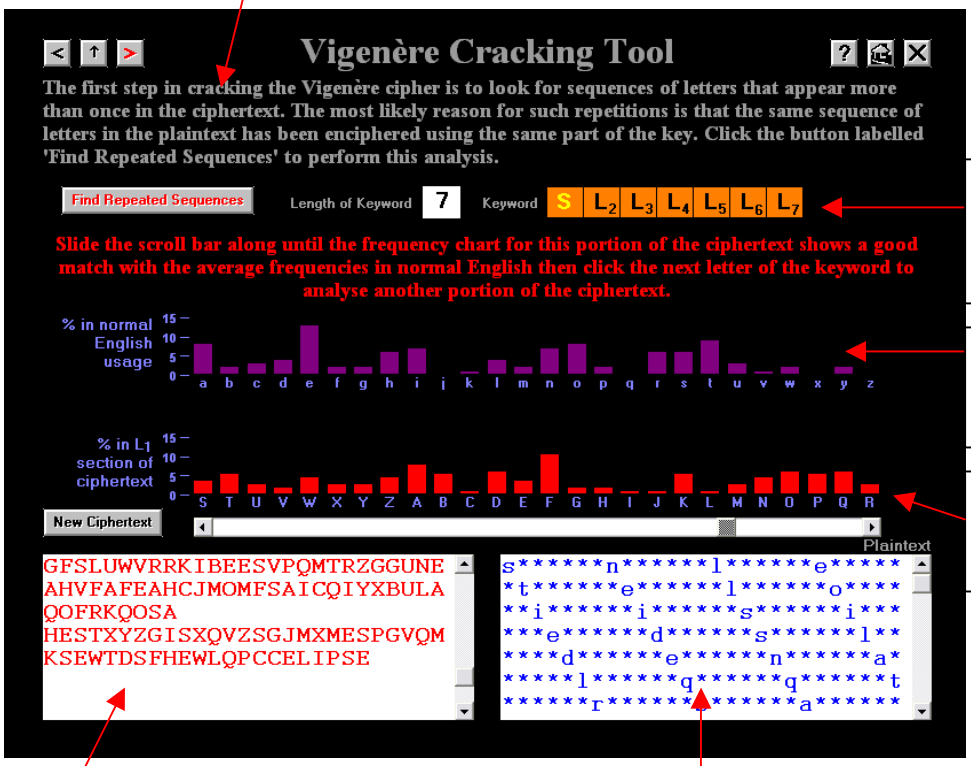
Nota: La operació per fer els percentages és $\frac{n^o\ repeticions}{465}\times 100$, on 465 és el total de lletres del text.

3. XIFRA DE VIGENÈRE

Les següents imatges són les captures de pantalla del programa “Los códigos secretos” d’en Simon Singh. En aquest apartat se soluciona el missatge xifrat amb Vigenère.

Com hem vist abans amb la captura de pantalla, la clau té 7 lletres. Cada lletra de la clau correspon a un alfabet i està indicada amb color taronja. En la part esquerra està el text xifrat i en la part dreta va apareixent el text en clar a mesura que es resol la clau. Cal fixar-se en els dígrafs catalans com “qu, gu, ss, rr, sc, ll, ny” ja que ens aporten pistes per saber si estem desxifrant correctament. La rigidesa del llenguatge ens ajudarà a trobar la solució. El programa també inclou un gràfic de barres amb la freqüència de les lletres en el text xifrat que es compara amb la freqüència de les lletres en anglès. Aquest últim no ens serveix perquè sabem que el text està escrit en català. Vaig elaborar un gràfic amb l’Excel de l’anàlisi de freqüència del català que es troba en l’apartat “anàlisi de freqüència”.

El primer pas en trencar la xifra Vigenère és mirar les seqüències de lletres que apareixen més d’un cop en el text xifrat. La raó més probable d’aquestes repeticions és que la mateixa seqüència de lletres en el text en clar ha estat xifrada usant la mateixa part de la clau. Premeu el botó etiquetat com “Troba seqüències repetides” per dur a terme aquest anàlisi.



Clau de 7 lletres. Primera lletra S. Mireu explicació sota la imatge.

Anàlisi de freqüència en anglès

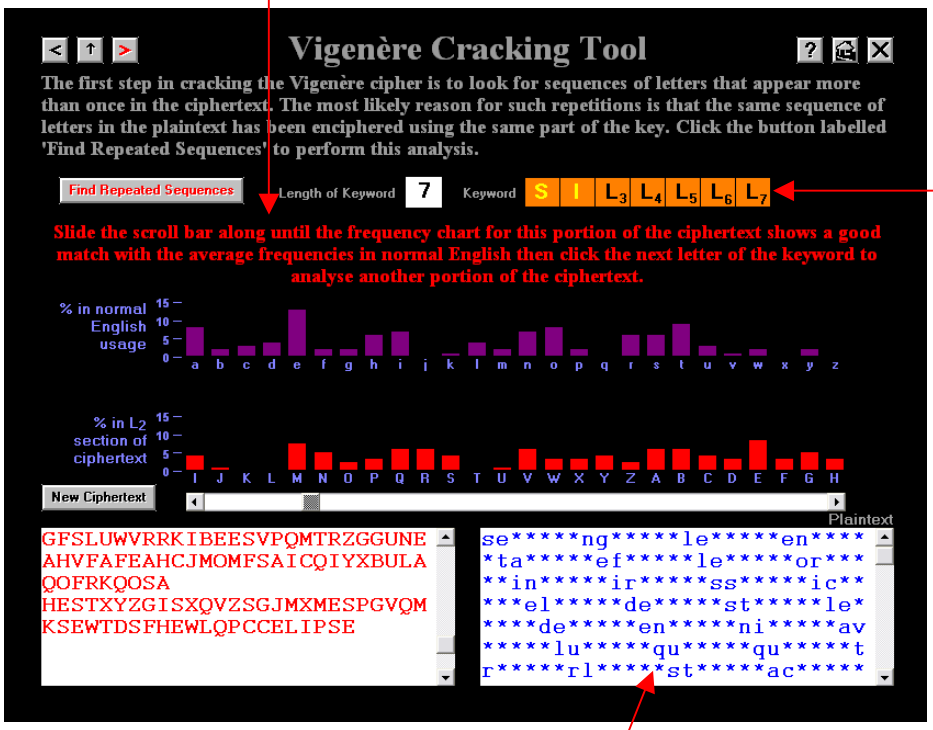
Anàlisi de freqüència del text xifrat

Text xifrat

Text en clar

Les lletres de la clau són les que després de molt de temps comparant gràfics de freqüència en català i del text xifrat em coincideixen per tal que el text en clar tingui sentit. Si el text fos en anglés seria molt visual en la imatge perquè les barres dels dos gràfics de freqüència de la captura de pantalla coincidirien.

Desplaça la barra desplegable fins que la freqüència del gràfic d'aquesta porció de text xifrat mostri una bona relació amb la mitjana de freqüències en anglés normal. Després feu *clic* en la següent lletra de la clau per analitzar una altra porció de text xifrat.

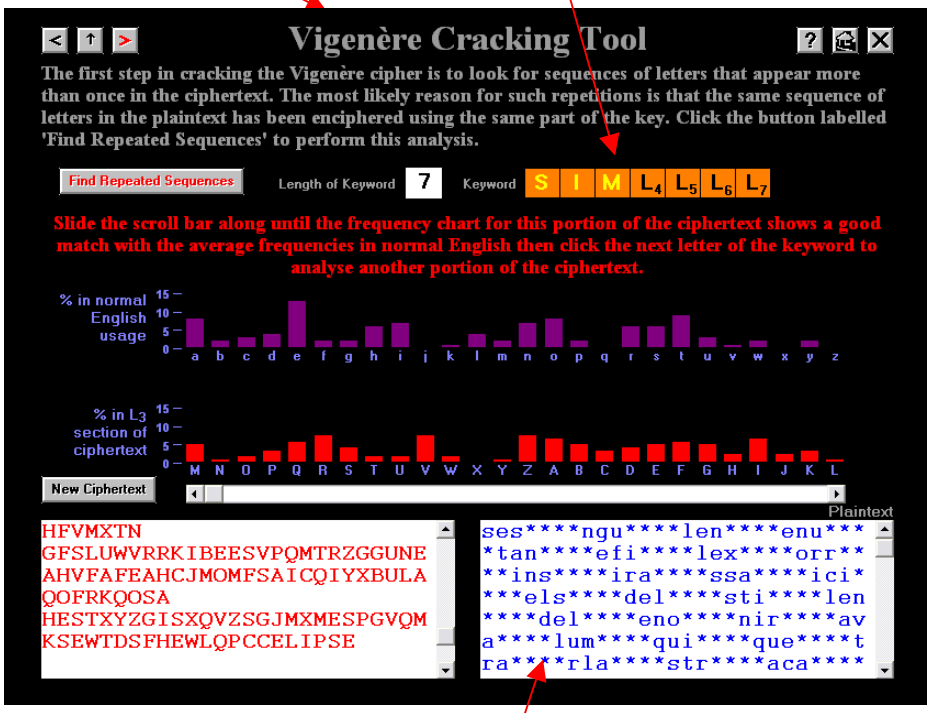


La lletra de la clau d'aquest pas és la I

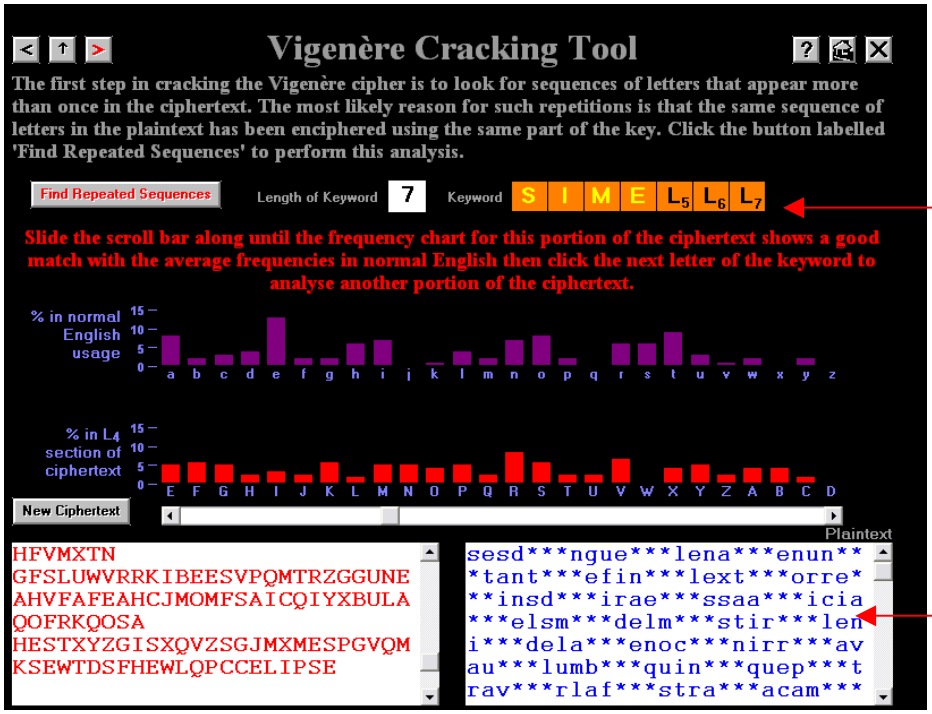
Es comencen a veure els primers dígrafs catalans (*qu*, *ss*) que ens indiquen que el desxiframent és correcte. També apareixen petites paraules molt freqüents com "de", "el".

Eina per trencar Vigenère

Nova lletra de la clau: M

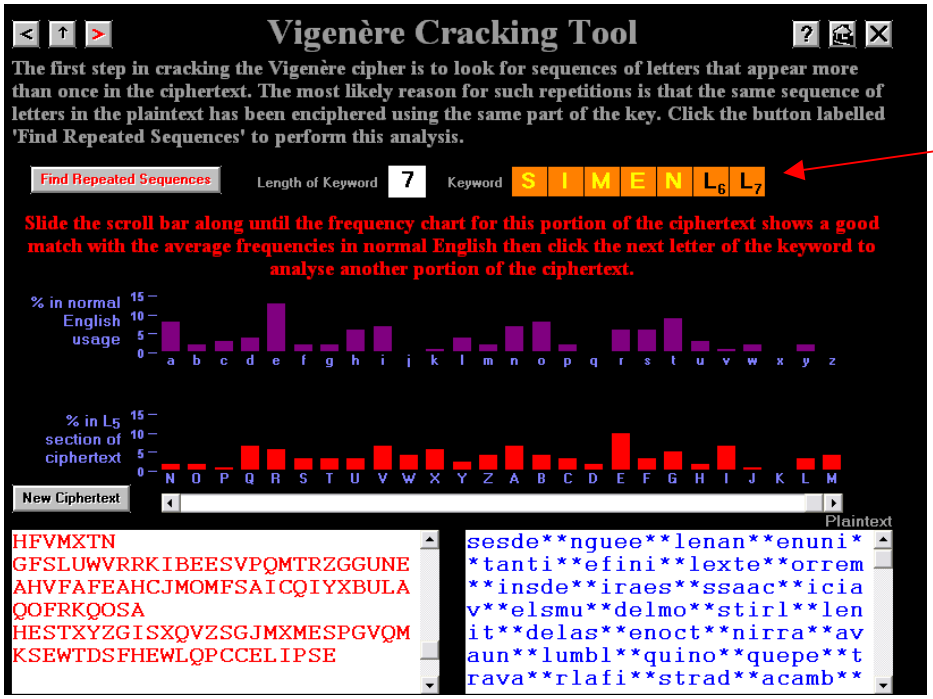


S'observen paraules com: *que*, *qui*, *els*, *dels*. També dígrafs acompanyats de vocals com "orr".

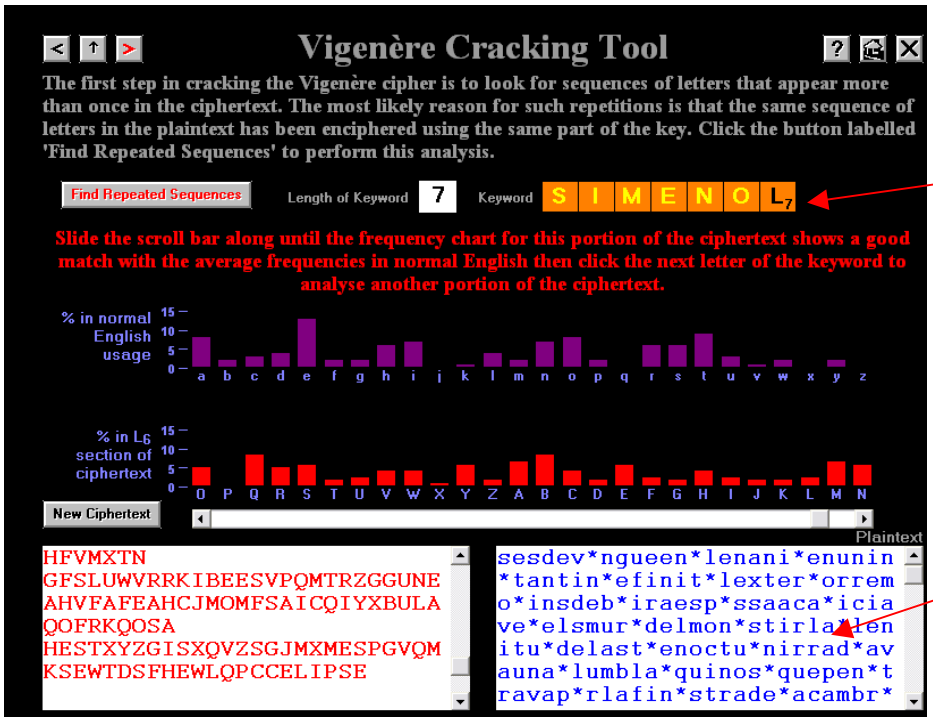


Nova lletra: E

Es comencen a distingir paraules amb sentit. La clau sembla ser correcta.

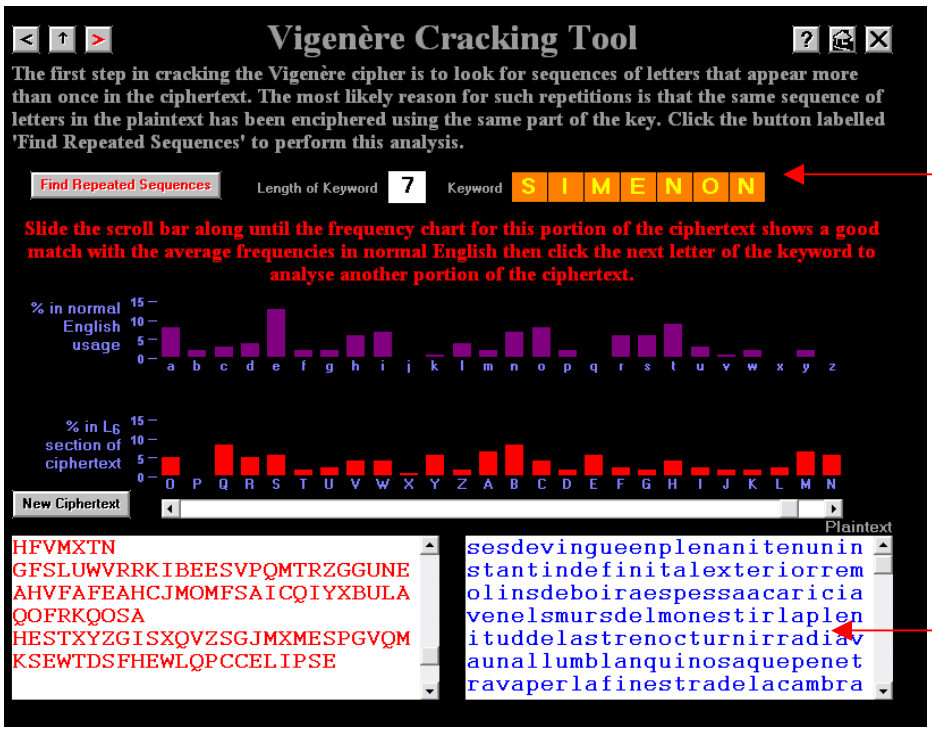


La N és la següent lletra.



Per lògica tocava una vocal

Text en clar gairebé resolt.



Clau: SIMENON

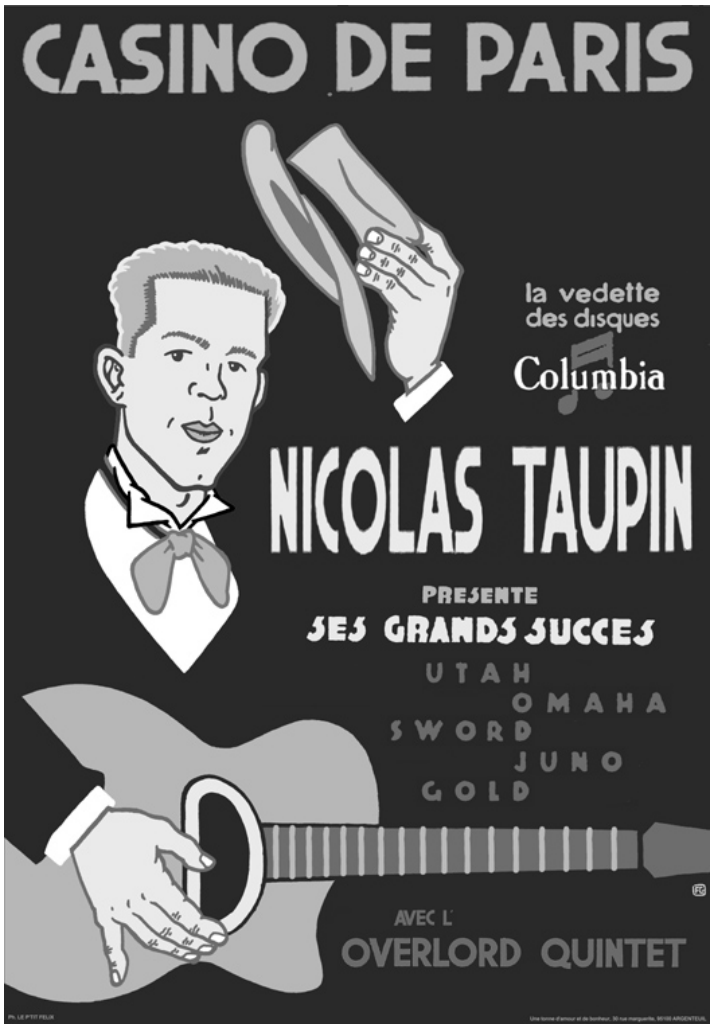
Text desxifrat

La clau del text és SIMENON i el text pla amb espais i signes de puntuació és el següent:

S'esdevingué en plena nit, en un instant indefinit. A l'exterior, remolins de boira espessa acariciaven els murs del monestir. La plenitud de l'astre nocturn irradiava una llum blanquinosa que penetrava per la finestra de la cambra. Els barrots metàl·lics tallaven el feix lumínic, que es projectava, quadriculat, al damunt d'un grup de quatre objectes. Des de l'altra banda de la porta un soroll sord i compassat, que tant podia provenir d'unes sandàlies d'espart com del frec d'una túnica o un hàbit, es desplacava pel passadís. El monjo rebutja d'entrada la hipòtesi d'una experiència onírica i va considerar que la lleugera flaire de cera cremada era un indici racional prou sòlid. Se sobreposà i decidí que només li feia por el Diable i que al dimoni no li calen espelmes. Obrí, doncs, el forrellat i sortí al corredor. Un floquet lumínic oscil·lant s'allunyava cap a les profunditats del passadís i desapareixia pel tombant, instant precís en què el joc d'ombres i contrallums va permetre-li reconèixer el rostre del portador.

Com a curiositat val a dir que és un fragment adaptat que en David Juher inclou en el primer capítol del seu llibre *L'art de la comunicació secreta*.

4. POSTER DE TAUPIN



ÍNDEX