

Cifrul Vigenère

În încercarea de a se lupta cu metoda analizei frecvenței, criptograful și diplomatul francez Blaise de Vigenère a propus în 1562 un criptosistem cu substituție polialfabetică. Sistemul de cifrare al lui Vigenère se bazează pe descoperirile matematicianului italian Leon Battista Alberti (născut în 1404), ale călugărului german Johannes Trithemius (născut în 1492) și ale omului de știință italian Giovanni Porta (născut în 1535). Sistemul acționează ca un cifru Caesar cu diferența că fiecare literă din textul simplu este criptată diferit în funcție de poziția pe care o ocupă aceasta în textul necifrat. Mai exact, se folosea pentru criptare și pentru decriptare un pătrat *Vigenère*, ce avea 26 de linii și 26 de coloane. Fiecare linie conține cele 26 de litere ale alfabetului translatate cu câte o poziție de la rând la rând, adică liniile și coloanele reprezintă câte un cifru Caesar cu cheile $0, 1, \dots, 25$. Dat un mesaj $m \in \Sigma^*$, se alege mai întâi o cheie $k \in \Sigma^*$, care este scrisă deasupra mesajului m simbol cu simbol, eventual repetând cheia (dacă aceasta este mai scurtă decât mesajul), până ce se ajunge la lungimea lui m . Astfel fiecare literă m_i din mesajul m este criptată ca la cifrul Caesar, folosind linia din pătratul Vigenère care începe cu litera k_i , unde k_i este litera aflată deasupra lui m_i .

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

Exemplul 1. Să presupunem că dorim să criptăm mesajul ”Gallia est omnis divisa in partes tres”, folosind cuvântul cheie BRUTUS. Pentru o mai mare siguranță în practică nu se iau în considerare spațiile goale. Așa cum am spus se repetă cuvântul cheie (punând-ul deasupra mesajului necriptat) până când textul simplu este acoperit în în tregime:

cheia	B, R, U, T, U, S	B, R, U, T, U, S	B, R, U, T, U, S	B, R, U, T, U, S	B, R, U, T, U, S	B, R
simplu	G, A, L, L, I, A	E, S, T, O, M, N	I, S, D, I, V, I	S, A, I, N, P, A	R, T, E, S, T, R,	E, S
cifrat	H, R, F, E, C, S	F, J, N, H, G, F	J, J, X, B, P, A	T, R, C, G, J, S	S, K, Y, L, N, J,	F, J

Să remarcăm că literele G și O sunt criptate prin aceeași literă (adică H) iar litera L este criptată prin litere diferite (F și E), deci nu mai este vorba de o simplă permutare a literelor. Astfel spargerea sistemului nu se mai poate face prin simpla analiză a frecvenței apariției literelor ca în cazul substituției monoalfabetice.

Ne propunem acum să formalizăm acum acest sistem.

Pentru un $n \in \mathbb{N}$ fixat, fie $K = M = C = \mathbb{Z}_{26}^n$. Mesajele $m \in \Sigma^*$, unde Σ este alfabetul limbii engleze, sunt împărțite în blocuri de lungime n și sunt criptate bloc cu bloc. Cifrul Vigenère se poate descrie acum astfel:

- Pentru fiecare $e \in K$ definim funcția de criptare $E_e : \mathbb{Z}_{26}^n \rightarrow \mathbb{Z}_{26}^n$ prin

$$E_e(m) = m + e \pmod{26},$$

unde adunarea se face simbol cu simbol modulo 26.

- Pentru fiecare $d \in K$ definim funcția de decriptare $D_d : \mathbb{Z}_{26}^n \rightarrow \mathbb{Z}_{26}^n$ prin

$$D_d(m) = m - d \pmod{26},$$

unde scăderea se face simbol cu simbol modulo 26.

Cifrul lui Vigenère a fost socotit sute de ani indecifrabil (apăruse doar cu un an înainte de moartea Mariei Stuart). Avantajul său era că nu avea nevoie de un nomenclator care trebuia păstrat secret, cuvântul cheie fiind reținut cu ușurință. Totuși are cel puțin două slăbiciuni evidente. Pe de o parte criptosistemul aplicat fiecărei litere este pur și simplu un cifru Caesar, pe de altă parte cheia se repetă după un număr relativ mic de pași.

Există mai multe metode de a sparge cifrul Vigenère. Prima persoană care a propus o astfel de metodă a fost Charles Babbage, cunoscut ca inventator al unor calculatoare mecanice în secolul al XIX-lea. Babbage nu a publicat niciodată descoperirea sa, și se speculează că a fost folosită de către Serviciile Secrete Britanice în războiul din Crimeea. Câțiva ani mai târziu, în 1863, un ofițer prusac pensionar Friedrich W. Kassiski, a reușit să dea o metodă similară de decifrare, care acum îi poartă numele. O altă metodă, numită testul Friedman, a fost inventată în 1920 de către William F. Friedman. Friedman a folosit indexul de coincidență, care măsoară frecvența neuniformă a literelor din textul cifrat.

Definiția 1. Fie $s = c_1 c_2 \dots c_n$ un șir de n litere (presupunem din alfabetul limbii engleze). Indicele de coincidență al lui s , notat cu $I_c(s)$, se definește ca fiind probabilitatea ca două caractere luate la întâmplare din s să fie identice.

Pentru ușurință identificăm literele A, B, C, \dots, Z cu numerele $0, 1, \dots, 25$.

Propoziția 1. Fie $s = c_1 c_2 \dots c_n$ un șir de n litere. Dacă f_i este frecvența cu care apare litera i în șirul s (de exemplu, dacă litera H apare de 23 de ori în secvența s , atunci $f_7 = 23$, a 7-a literă din alfabet fiind H) atunci indicele de coincidență se calculează după formula

$$I_c(s) = \frac{1}{n(n-1)} \sum_{i=0}^{25} f_i(f_i - 1).$$

Demonstrație: Putem alege două elemente la întâmplare din s în C_n^2 moduri. Pentru fiecare i , $0 \leq i \leq 25$, există $C_{f_i}^2$ moduri de alege două litere din s care să fie egale cu i și deci numărul total de moduri în care putem alege două caractere egale este $\frac{1}{2} \sum_{i=0}^{25} f_i(f_i - 1)$. Obținem astfel formula:

$$I_c(s) = \frac{1}{n(n-1)} \sum_{i=0}^{25} f_i(f_i - 1).$$

□

Exemplul 2. 1. Dacă s este secvența "Rats live on no evil star" atunci indicele de coincidență este $I_c(s) = \frac{1}{20 \cdot 19}(10 \cdot (2 \cdot 1)) = \frac{1}{19} = 0,052$.

2. Dacă t este secvența "A man a plan a canal panama" atunci indicele de coincidență este $I_c(t) = \frac{1}{21 \cdot 20}(10 \cdot 9 + 3(2 \cdot 1) + 4 \cdot 3 + 1 \cdot 0) = \frac{108}{420} = 0,257$.

$I_c(t)$ este foarte mare pentru că sunt (neobișnuit) de multe litere de a .

Să remarcăm acum că dacă secvența s este formată din n caractere alese la întâmplare, atunci $f_i = \frac{n}{26}$ și deci:

$$\begin{aligned} I_c(s) &= \frac{1}{n(n-1)} \sum_{i=0}^{25} \frac{n}{26} \left(\frac{n}{26} - 1 \right) = \\ &= \frac{26}{n(n-1)} \frac{n}{26} \left(\frac{n}{26} - 1 \right) = \frac{\frac{n}{26} - 1}{n-1} \approx \frac{1}{26} \approx 0,0385. \end{aligned}$$

Pe de altă parte, dacă s este un text în limba engleză, atunci folosind tabele de frecvența apariției literelor se poate arăta că indicele de coincidență este $I_c(s) \approx 0,0685$.

Ținând seama că substituția monoalfabetică se face folosind permutări ale alfabetului, indicele de coincidență al textului criptat nu se va modifica. În acest caz, probabilitățile individuale se vor permuta, dar indicele va rămâne neschimbat. Dacă indicele de coincidență al unui text criptat este apropiat de valoarea 0,0685 atunci sunt șanse ca să fie o substituție simplă monoalfabetică în limba engleză. Dacă în schimb $I_c(s)$ al unui text criptat este apropiat de valoarea 0,0385 atunci sunt șanse să avem un text cu litere alese la întâmplare, care nu satisfac regulile statistice ale frecvenței apariției literelor, deoarece probabilitatea ca două caractere să fie egale este tot $\frac{1}{26}$.

Criptanaliza cifrului Vigenère se face în doi pași. Mai întâi se găsește lungimea cheii. Acest lucru poate fi făcut prin două moduri (care se pot completa unul pe celălalt), metoda lui Kasiski și folosind indicele de coincidență din testul Friedman.

Prima etapă în procesul de criptanaliză al lui Kasiski este de a căuta șiruri de litere care se repetă în textul cifrat. Există două motive pentru care asemenea repetiții pot apărea. Cel mai probabil este că același șir de litere din textul în clar a fost cifrat folosindu-se aceeași parte a cuvântului cheie. Există de asemenea posibilitatea mai puțin probabilă ca două șiruri diferite de litere din textul în clar să fi fost cifrate folosindu-se părți diferite din cuvântul cheie, conducând din întâmplare la șiruri identice în textul cifrat. Dacă ne limităm la șirurile lungi, atunci a doua posibilitate se reduce considerabil. În practică ne uităm după grupuri de trei sau patru litere care se repetă și măsurăm distanța dintre ele. Apoi un factor comun al majorității distanțelor (nu neapărat al tuturor). Acesta are șanse să fie lungimea cheii, să zicem k .

Putem verifica dacă valoarea găsită este corectă folosind indicii de coincidență.

Presupunem acum că $s = c_1 c_2 \dots c_n$ este un string obținut printr-o criptare cu un cifru Vigenère. Oscar (atacatorul) va împărți stringul c în substringurile s_i , $1 \leq i \leq k$:

$$s_i = c_i c_{i+k} c_{i+2k} c_{i+3k} \dots,$$

unde k este o posibilă lungime a cheii folosită pentru criptare. Să remarcăm că dacă Oscar a ghicit corect lungimea k a cheii folosită pentru criptare, atunci fiecare s_i este obținut printr-o criptare cu câte un cifru Caesar și deci literele sale se vor supune frecvențelor știute din

limba engleză. Pe de altă parte, dacă Oscar a ghicit incorect, stringurile s_i vor fi mai mult sau mai puțin aleatoare. Astfel pentru fiecare k , Oscar calculează $I_c(s_i)$, pentru $1 \leq i \leq k$ și verifică dacă aceste numere sunt mai apropiate de 0,065 sau de 0,038. El calculează indicii de coincidență pentru $k = 3, 4, 5, \dots$ până când găsește o valoare a lui k pentru care valoarea medie a $I_c(s_1), I_c(s_2), \dots, I_c(s_k)$ devine mare (să zicem mai mare decât 0,06). Atunci acest k este probabil lungimea cheii de criptare.

Să vedem acum cum funcționează cele două metode pe un exemplu concret.

Presupunem că am interceptat următorul text cifrat despre care știm că fost criptat cu cifrul Vigenère.

zpgdl rjlaj kpylx zpyyg lrjgd lrzhz qyjqz repvm swrzy rigzh
zvreg kwivs saolt nliuw oldie aqewf iyykh bjowr hdogc qhkwa
jyagg emisr zqoqh oavlk bjofr ylvps rtgiu avmsw lzgms evwpc
dmjsv jqbrn klpcf iowhv kxjbj pmfkr qthtk ozrgq ihbmq sbivd
ardym qmpbu nivxm tzwqv gefjh ucbor vwped xuwft qmoow jipds
fluqm oeavl jgqea lrkti wvext vkrrg xani

În tabelul de mai jos sunt date grupurile de trei litere care se repetă, poziția precum și distanțele dintre aceste apariții.

Grupuri de trei litere	Poziția	Distanța
avl	117 și 258	$141 = 3 \cdot 47$
bjo	86 și 121	$35 = 5 \cdot 7$
dlr	4 și 25	$21 = 3 \cdot 7$
gdl	3 și 24	$16 = 2^4$
lrj	5 și 21	$98 = 2 \cdot 7^2$
msw	40 și 138	$84 = 2^2 \cdot 3 \cdot 7$
pcd	149 și 233	$13 = 13$
qmo	241 și 254	$98 = 2 \cdot 7^2$
vms	39 și 137	$84 = 2^2 \cdot 3 \cdot 7$
vwp	147 și 231	$84 = 2^2 \cdot 3 \cdot 7$
wpc	148 și 232	$21 = 3 \cdot 7$
zhz	28 și 49	$21 = 3 \cdot 7$

Majoritatea numerelor din ultima coloană sunt divizibile cu 7 și deci, urmând metoda lui Kasiski, putem presupune că lungimea cheii este chiar 7.

Deși testul Kasiski ne arată că perioada este probabil 7, vom aplica și testul indicelui de coincidență pentru a vedea cum funcționează.

Tabelul de mai jos listează indicii de coincidență pentru diferite alegeri ale lungimii cheilor.

Lungimea cheii	Media indicilor	Indicele individual de coincidență
4	0.038	0.034, 0.042, 0.039, 0.035
5	0.037	0.038, 0.039, 0.043, 0.027, 0.036
6	0.036	0.038, 0.038, 0.039, 0.038, 0.032, 0.033
7	0.062	0.062, 0.057, 0.065, 0.059, 0.060, 0.064, 0.064
8	0.038	0.037, 0.029, 0.038, 0.030, 0.034, 0.057, 0.040, 0.039
9	0.037	0.032, 0.036, 0.028, 0.030, 0.026, 0.032, 0.045, 0.047, 0.056

Observăm că dacă lungimea cheii este 7, obținem cel mai mare indice de coincidență, ceea ce ne confirmă concluzia testului Kasiski.

Să explicăm acum cum funcționează metoda lui Friedman de aflare a cheii după ce știm lungimea acesteia. Metoda constă în compararea stringurilor s_1, s_2, \dots, s_k fiecare cu fiecare. Instrumentul folosit pentru a compara diferite stringuri se numește indicele mutual de coincidență. Ideea generală este aceea că fiecare din cele k stringuri a fost criptat folosind câte un cifru Caesar. Dacă translația făcută pentru stringul s_i este β_i iar pentru stringul s_j este β_j , atunci ne așteptăm ca frecvențele legate de s_i să se potrivească mai bine cu cele ale lui s_j atunci când simbolurile din s_i sunt translatate cu o cantitate suplimentară egală cu $\beta_j - \beta_i \pmod{26}$. Acest lucru ne conduce la următoarea definiție:

Definiția 2. Fie $s = c_1 c_2 \dots c_n$ și $t = d_1 d_2 \dots d_m$ două stringuri de caractere alfabetice. Indicele mutual de coincidență al lui s și t , notat cu $IM_c(s, t)$, este probabilitatea ca un caracter ales aleator din s să coincidă cu un caracter ales aleator din t .

Dacă notăm cu $f_i(s)$ numărul de apariții ale literei i în stringul s și cu $f_i(t)$ numărul de apariții ale literei i în stringul t , atunci probabilitatea de a alege litera i din cele două stringuri este produsul probabilităților $\frac{f_i(s)}{n}$ și $\frac{f_i(t)}{m}$. Avem astfel formula

$$IM_c(s, t) = \frac{1}{nm} \sum_{i=0}^{25} f_i(s) f_i(t).$$

Indicele mutual de coincidență are proprietăți asemănătoare cu cele ale indicelui de coincidență. Valoarea lui $IM_c(s, t)$ poate fi folosită pentru a confirma sau infirma dacă mărimea translației ghicite este corectă. Astfel, dacă două stringuri s și t sunt criptate folosind același cifru cu substituție simplă, atunci $IM_c(s, t)$ tinde să aibă o valoare mare datorită frecvenței neuniforme cu care apar literele. Pe de altă parte, dacă stringurile s și t sunt criptate cu cifruri diferite, atunci nu există vreo relație între ele, și indicele mutual de coincidență va fi mult mai mic.

Ne întoarcem la atacul lui Oscar asupra cifrului Vigenère. El cunoaște lungimea cheii și împarte textul cifrat în k blocuri s_1, s_2, \dots, s_k . Literele din fiecare bloc s_i au fost obținute prin translatarea cu aceeași mărime β_i . Pasul următor al lui Oscar este să compare pe s_i cu stringul $s_j + \sigma$, obținut din s_j prin translatarea la stânga cu diferite mărimi σ . Dacă se întâmplă ca σ să fie egală cu $\beta_i - \beta_j$, atunci $s_j + \sigma$ a fost translatat cu $\beta_j + \sigma$ poziții față de textul în clar și deci $s_j + \sigma$ și s_i au fost criptate folosind aceeași translație. Astfel indicii lor mutuali de coincidență vor fi foarte mari. Pe de altă parte, dacă σ nu este egală cu $\beta_i - \beta_j$, atunci $s_j + \sigma$ și s_i au fost criptați prin translații diferite și deci $IM_c(s, t)$ tinde să fie foarte mic. Astfel, Oscar calculează indicii mutuali de coincidență

$$IM_c(s_i, s_j + \sigma), \text{ pentru } 1 \leq i < j \leq k \text{ și } 0 \leq \sigma \leq 25.$$

După ce Oscar urmărește toate aceste valori, selectează pe acelea care sunt suficient de mari (să presupunem mai mari decât 0,65). Fiecare valoare mare a lui $IM_c(s_i, s_j + \sigma)$ face ca să avem egalitățile

$$\beta_i - \beta_j \equiv \sigma \pmod{26}. \quad (1)$$

Aceasta conduce la un sistem de ecuații de forma 1 în variabilele $\beta_1, \beta_2, \dots, \beta_k$. În practică unele din aceste ecuații s-ar putea să nu fie adevărate, dar după câteva încercări, Oscar va obține valorile $\gamma_2, \dots, \gamma_k$ ce satisfac

$$\beta_2 = \beta_1 + \gamma_2, \beta_3 = \beta_1 + \gamma_3, \dots, \beta_k = \beta_1 + \gamma_k$$

Asfel, dacă se întâmplă ca cheia să înceapă cu litera A , atunci a doua literă va fi A translatat cu γ_2 poziții, a treia literă din cheie va fi A translatat cu γ_3 poziții, și așa mai departe, dacă cheia se întâmplă să înceapă cu litera B , atunci a doua literă va fi B translatat cu γ_2 poziții, a treia literă din cheie va fi B translatat cu γ_3 poziții, și așa mai departe. Oscar nu are acum decât să încerce toate cele 26 de cuvinte cheie corespunzătoare.

Ne întoarcem acum la exemplul nostru. Oscar știe că lungimea cheii este 7 și împarte textul cifrat în șapte blocuri luând mereu a șaptea literă:

$s_1 = \text{zlxrrrhwoehdweoklilwvlhphqbynhwfwjulrxx}$
 $s_2 = \text{pazjzezzitlwboamqbvuzpjpvmtiimiquptiqjka}$
 $s_3 = \text{gjpgqpyvvndfjgjhjpagcckfkfkhvqvccqpmgtvn}$
 $s_4 = \text{dkydyvrrsliocysoosvmdbfxkobdmxgbdmdoqiki}$
 $s_5 = \text{lpyljmiesieiwqarafrmsmrijrzmameoxoseewr}$
 $s_6 = \text{rygrzsggauayrhgzvrtsejnobqqrqbtfruofaavr}$
 $s_7 = \text{jllzqwzkowqkhkgqlygwvskwtjgsduzjvwwlvleg}$

Să observăm că primele șapte litere se află pe prima coloană, următoarele șapte pe a doua coloană și așa mai departe. Apoi el va compara blocul s_i cu blocul s_j translatat (la stânga) cu σ poziții (pe care-l notăm cu $s_j + \sigma$) luând pe rând $\sigma = 0, 1, 2, \dots, 25$. Tabelele de mai jos ne dau listele complete ale indicilor mutuali de coincidență $IM_c(s_i, s_j + \sigma)$, $1 \leq i < j \leq 7$ și $0 \leq \sigma \leq 25$. Dacă indicele este mare, sunt șanse mari ca s_j să fie translatat față de s_i cu σ poziții. Dacă notăm ca mai sus cu β_i mărimea translației cu care a fost obținut s_i , atunci valoarea mare (mai mare decât 0,065) a indicilor subliniați face ca să presupunem că $\beta_i - \beta_j = \sigma$.

i	j	0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	.025	.034	.045	.049	.025	.032	.037	.042	.049	.031	.032	.037	.043
1	3	.023	<u>.067</u>	.055	.022	.034	.049	.036	.040	.040	.046	.025	.031	.046
1	4	.032	.041	.027	.040	.045	.037	.045	.028	.049	.042	.042	.030	.039
1	5	.043	.021	.031	.052	.027	.049	.037	.050	.033	.033	.035	.044	.030
1	6	.037	.036	.030	.037	.037	.055	.046	.038	.035	.031	.032	.037	.032
1	7	.054	.063	.034	.030	.034	.040	.035	.032	.042	.025	.019	.061	.054
2	3	.041	.029	.036	.041	.045	.038	.060	.031	.020	.045	.056	.029	.030
2	4	.028	.043	.042	.032	.032	.047	.035	.048	.037	.040	.028	.051	.037
2	5	.047	.037	.032	.044	.059	.029	.017	.044	.060	.034	.037	.046	.039
2	6	.033	.035	.052	.040	.032	.031	.031	.029	.055	.052	.043	.028	.023
2	7	.038	.037	.035	.046	.046	.054	.037	.018	.029	.052	.041	.026	.037
3	4	.029	.039	.033	.048	.044	.043	.030	.051	.033	.034	.034	.040	.038
3	5	.021	.041	.041	.037	.051	.035	.036	.038	.025	.043	.034	.039	.036
3	6	.037	.034	.042	.034	.051	.029	.027	.041	.034	.040	.037	.046	.036
3	7	.046	.023	.028	.040	.031	.040	.045	.039	.020	.030	<u>.069</u>	.042	.037
4	5	.041	.033	.041	.038	.036	.031	.056	.032	.026	.034	.049	.029	.054
4	6	.035	.037	.032	.039	.041	.033	.032	.039	.042	.031	.049	.039	.058
4	7	.031	.032	.046	.038	.039	.042	.033	.056	.046	.027	.027	.036	.036
5	6	.048	.036	.026	.031	.033	.039	.037	.027	.037	.045	.032	.040	.041
5	7	.030	.051	.043	.031	.034	.041	.048	.032	.053	.037	.024	.029	.045
6	7	.032	.033	.030	.038	.032	.035	.047	.050	.049	.033	.057	.050	.021

i	j	13	14	15	16	17	18	19	20	21	22	23	24	25
1	2	.034	.052	.037	.030	.037	.054	.021	.018	.052	.052	.043	.042	.046
1	3	.031	.037	.038	.050	.039	.040	.026	.037	.044	.043	.023	.045	.032
1	4	.039	.040	.032	.041	.028	.019	<u>.071</u>	.038	.040	.034	.045	.026	.052
1	5	.042	.032	.038	.037	.032	.045	.045	.033	.041	.043	.035	.028	.063
1	6	.040	.030	.028	<u>.071</u>	.051	.033	.036	.047	.029	.037	.046	.041	.027
1	7	.040	.032	.049	.037	.035	.035	.039	.023	.043	.035	.041	.042	.027
2	3	.054	.040	.028	.031	.039	.033	.052	.046	.037	.026	.028	.036	.048
2	4	.047	.034	.027	.038	.047	.042	.026	.038	.029	.046	.040	.061	.025
2	5	.034	.026	.035	.038	.048	.035	.033	.032	.040	.041	.045	.033	.036
2	6	.033	.034	.036	.036	.048	.040	.041	.049	.058	.028	.021	.043	.049
2	7	.042	.037	.041	.059	.031	.027	.043	.046	.028	.021	.044	.048	.040
3	4	.037	.045	.033	.028	.029	<u>.073</u>	.026	.040	.040	.026	.043	.042	.043
3	5	.035	.029	.036	.044	.055	.034	.033	.046	.041	.024	.041	<u>.067</u>	.037
3	6	.023	.043	<u>.074</u>	.047	.033	.043	.030	.026	.042	.045	.032	.035	.040
3	7	.035	.035	.035	.028	.048	.033	.035	.041	.038	.052	.038	.029	.062
4	5	.032	.041	.036	.032	.046	.035	.039	.042	.038	.034	.043	.036	.048
4	6	.034	.034	.036	.029	.043	.037	.039	.036	.039	.033	<u>.066</u>	.037	.028
4	7	.043	.032	.039	.034	.029	<u>.071</u>	.037	.039	.030	.044	.037	.030	.041
5	6	.052	.035	.019	.036	.063	.045	.030	.039	.049	.029	.036	.052	.041
5	7	.040	.031	.034	.052	.026	.034	.051	.044	.041	.039	.034	.046	.029
6	7	.029	.035	.039	.032	.028	.039	.026	.036	<u>.069</u>	.052	.035	.034	.038

Pasul următor este să se rezole sistemul de ecuații (în necunoscutele β_1, \dots, β_7) din ultima coloană a tabelului de mai jos. Să reamintim că toate ecuațiile sunt modulo 26.

i	j	σ	IM_c	
1	3	1	0.067	$\beta_1 - \beta_3 = 1$
3	7	10	0.069	$\beta_3 - \beta_7 = 10$
1	4	19	0.071	$\beta_1 - \beta_4 = 19$
1	6	16	0.071	$\beta_1 - \beta_6 = 16$
3	4	18	0.073	$\beta_3 - \beta_4 = 18$
3	5	24	0.067	$\beta_3 - \beta_5 = 24$
3	6	15	0.074	$\beta_3 - \beta_6 = 15$
4	6	23	0.066	$\beta_4 - \beta_6 = 23$
4	7	18	0.071	$\beta_4 - \beta_7 = 18$
6	7	21	0.069	$\beta_6 - \beta_7 = 21$

Se obțin cu ușurință relațiile

$$\beta_3 = \beta_1 + 25, \beta_4 = \beta_1 + 7, \beta_5 = \beta_1 + 1, \beta_6 = \beta_1 + 10, \beta_7 = \beta_1 + 15 \quad (2)$$

Nu avem încă informații despre β_2 . Ne uităm în tabelul indicilor și căutăm cele mai mari valori legate de blocul al doilea. Acestea sunt $(i, j) = (2, 3)$ cu mărimea translației egală cu 6 ($IM_c(2, 3) = 0, 060$) și $(i, j) = (2, 4)$ cu mărimea translației egală cu 24 ($IM_c(2, 3) = 0, 061$). Acestea ne dau relațiile

$$\beta_2 - \beta_3 = 6, \text{ și } \beta_2 - \beta_4 = 24.$$

Dacă înlocuim aceste ultime relații în (2) obținem $\beta_2 = \beta_1 + 5$.

Astfel, Oscar știe acum că indiferent de mărimea translației cu care a fost obținut s_1 , blocurile s_2, s_3, \dots, s_7 sunt translatate cu 5, 25, 7, 1, 10 și respectiv 15 poziții față de s_1 . Urmează acum să încerce toate cele 26 de valori posibile ale lui β_1 până obține un text în clar plauzibil.

β_1	cheie	text decriptat
0	AFZHBKP	zkhwhulvkdoowxuqrxwwrehwkhkhurripbrzqolih
1	BGAICLQ	yjgvjgtkujcnnvwtpqwvvqdgvgjgtqqhoaqpnhg
2	CHBJDMR	xifuifstibmmuvsopvuupcfuifisppgnzpxomjgf
3	DICKENS	whetherishallturnouttobettheheroofmyownlife
4	EJDLFOT	vgdsgdqhrzkkstqmntssnadsgdgdqnnelxnmkhed
5	FKEMGPU	ufcrfcpgqfyjjrsplmsrmzcrfcfcpmmdkwmuljdc
6	GLFNHQV	tebqebfofexiiqroklrqqlbqebebolcejvltkifcb
7	HMGOWRW	sdapdaneodwhhpqjnkppkxapdadankkbiuksjheba
8	INHPJSX	rczoczmdncvvgopmijpoojwzoczczmjjahtjrigdaz
.

Nu e greu de văzut că pentru $\beta_1 = 3$ se obține cheia DICKENS care duce la decifrarea:

wheth erish alltu rnout tobet heher oofmy ownli feorw hethe rthat stati onwil lbehe ldbya
nybod yelse these pages musts howto begin mylif ewith thebe ginni ngofin ylife ireco rdtha tiwas
borna sihav ebeen infor medan dbeli eveon afrid ayatt welve ocloc katni ghtit wasre marke dthat
thecl ockbe ganto strik eandi began tocry simul taneo usly

Iar după respațiere și punând semnele de punctuație vom obține:

Whether I shall turn out to be the hero of my own life, or whether that station will be
held by anybody else, these pages must show. To begin my life with the beginning of my life,
I record that I was born (as I have been informed and believe) on a Friday, at twelve o'clock at
night. It was remarked that the clock began to strike, and I began to cry, simultaneously.

(David Copperfield, 1850, Charles Dickens)