CURS 4
CIFRUL VIGÈNERE

Un **cifru de tip substituție polialfabetică** este o generalizare a sistemului de cifrare cu substituție monoalfabetică folosind mai multe alfabete, fiecare alfabet fiind o permutare a alfabetului de intrare. Algoritmul de cifrare constă în substituirea unei literei din textul clar cu litera corespunzătoare dintr-un anumit alfabet.

Cifrul Vigènere este un cifru simetric de tip substituție polialfabetică cu cheie secretă inventat în anul 1553 de către Giovan Battista Bellaso, dar atribuit, în mod eronat, lui Blaise de Vigenère care în 1586 a inventat un sistem de cifrare asemănător. Cifrul Vigènere a rezistat atacurilor criptanaliștilor peste 3 secole, fiind spart abia în anul 1863 de către Friedrich Wilhelm Kasiski.

Cifrul Vigènere utilizează, pentru realizarea substituției polialfabetice, o **tabelă Vigènere** și o cheie secretă:

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Criptarea unui mesaj se realizează astfel:

- se repetă cheia secretă până când se acoperă tot textul clar;
- fiecare literă din textul clar se criptează prin litera aflată la intersecția dintre linia corespunzătoare literei din textul clar și coloana corespunzătoare literei din cheia secretă în tabela Vigènere.

Text clar	I N A M I C U L V I N E D I N S U D
Cheia secretă	S E C R E T S E C R E T S E C R E T
Text cifrat	**A R C D M V M P X Z R X V M P J Y W**

Decriptarea unui mesaj se realizează astfel:

- se repetă cheia secretă până când se acoperă tot textul criptat;
- fiecare literă din textul criptat se decriptează determinând linia pe care apare litera din textul criptat pe coloana corespunzătoare literei din cheia secretă în tabela Vigènere.

Text cifrat	A R C D M V M P X Z R X V M P J Y W
Cheia secretă	S E C R E T S E C R E T S E C R E T
Text clar	**I N A M I C U L V I N E D I N S U D**

Considerând textul clar $P = p_0 p_1 \dots p_{n-1}$, textul criptat $C = c_0 c_1 \dots c_{n-1}$ și cheia secretă $K = k_0 k_1 \dots k_{m-1}$, procesele de criptare și decriptare pot fi definite matematic astfel:

$$c_i = (p_i + k_{i \bmod m}) \bmod 26$$
$$p_i = (c_i - k_{i \bmod m}) \bmod 26$$

Criptare			
i	p_i	$k_{i \bmod m}$	c_i
0	I = 8	S = 18	(8+18) mod 26 = 0 = A
1	N = 13	E = 4	(13+4) mod 26 = 17 = R
2	A = 0	C = 2	(0+2) mod 26 = 2 = C
3	M = 12	R = 17	(12+17) mod 26 = 3 = D
4	I = 8	E = 4	(8+4) mod 26 = 12 = M
5	C = 2	T = 19	(2+19) mod 26 = 21 = V
6	U = 20	S = 18	(20+18) mod 26 = 12 = M
7	L = 11	E = 4	(11+4) mod 26 = 15 = P
8	V = 21	C = 2	(21+2) mod 26 = 23 = X
⋮	⋮	⋮	⋮

Decriptare			
i	c_i	$k_{i \bmod m}$	p_i
0	A = 0	S = 18	(0-18) mod 26 = 8 = I
1	R = 17	E = 4	(17-4) mod 26 = 13 = N
2	C = 2	C = 2	(2-2) mod 26 = 0 = A
3	D = 3	R = 17	(3-17) mod 26 = 12 = M
4	M = 12	E = 4	(12-4) mod 26 = 8 = I
5	V = 21	T = 19	(21-19) mod 26 = 2 = C
6	M = 12	S = 18	(12-18) mod 26 = 20 = U
7	P = 15	E = 4	(15-4) mod 26 = 11 = L
8	X = 23	C = 2	(23-2) mod 26 = 21 = V
⋮	⋮	⋮	⋮

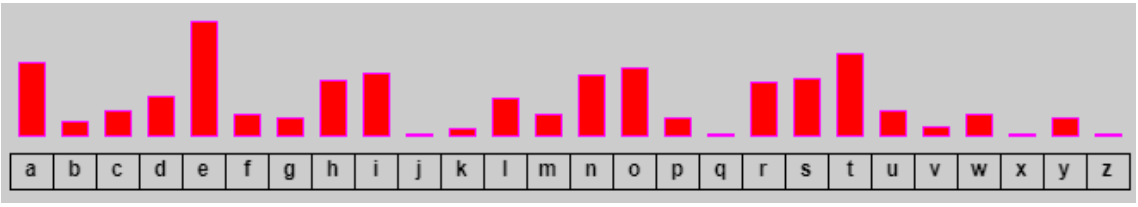
CRIPTANALIZA CIFRULUI VIGÈNERE

Software online:
https://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html

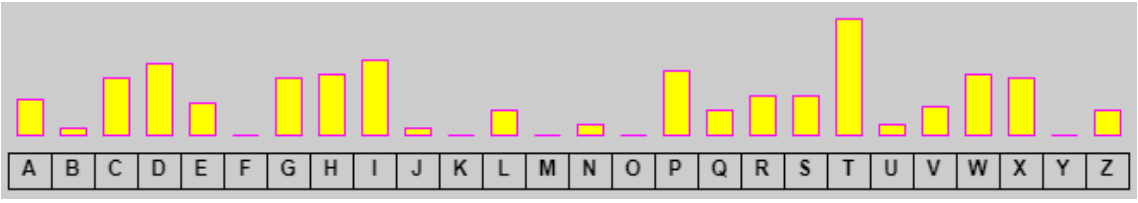
1. **Presupunând faptul că se cunoaște lungimea cheii secrete, se împarte textul cifrat pe un număr de coloane egal cu lungimea cheii secrete:**

IHWXEFJW	APZSXSKV	RRALEQRO	WENACSEH	HWALYVTL
LEDDZCTX	PFLWNGVY	ROEHKBVQ	GEUALVVU	EHWJWZGK
BEFLARUH	TRSDSCIG	IOXLDSML	LAKGNWXL	PBWLOSMH
HCJALHZR	HAFVOKZW	VEFWNSTL	CADDURVV	GYDWPHVU
COXSLCCB	RHWKSSIH	EHWJPVVW	RRATARSB	LHWJAOJD
PLHZWPVW	XNVAYOKH	GILZAAZX	VIGNWBSD	ABWJPWRQ
XCUALVVU	SBQONWKL	HCAHDSIK	ITAKPOSH	STJAPVVP
LAKXKFDX	CGLZAZVW	DWWNAFFQ	ALSKKWEK	XUKMOSUD
AALWZPPO	IEJGBHYH	AYHJKJZG	XSTGKYCD	UIPWZDRW
TOFTWHKL	ROJJAGGR	TDSHNCXU	RIXJWRVO	IEJFKTJX
HTSSHPVU	CDAFCOCS	TSKARSIL	HIYYECMD	QSLAPIKL
IISJKIEG	WATWPWEW	VIVSJRGU	CBSLPWJW	DNKTAZCD
PNVMOSUD	WEUALVVU	TDAUPOSO	PBWDHOJR	HOKKYVVP
BELSHQZS	IEPLHOKH	TSQKPSDI	WETMEZKX	TMWSJHKK
WEJVEGTW	GIFBKVRQ	DRKOEHTK	EOFLDSKD	TPSLPSIQ
DSOAPQYE	CEKLNWKK	XNYTAHNH	QUDSNSTW	DFKMXGKL
TTOWABTL	TMAMOWEK	TNUALVVU	POXLNWKK	IULAKBJF
EHWJWZGK	XSOGNYGR	PLHZWPVW	TMAMOPLW	DUDVXSVD
PBWLOOCE	AIYJWDYL	HCALWHZR	PDVWZOIH	....

2. **Fiecare coloană este un cifru Cezar, care poate fi spart folosind frecvența caracterelor:**

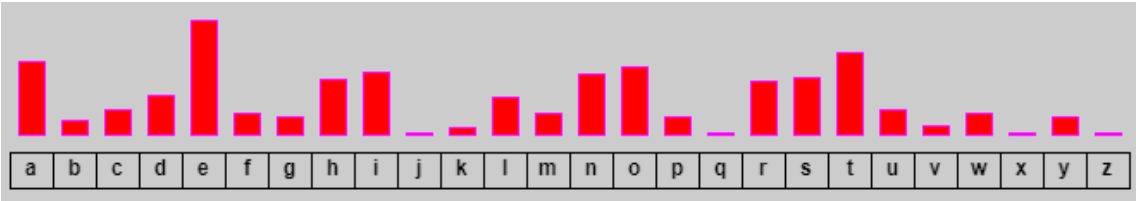


Frecvențele literelor din limba engleză

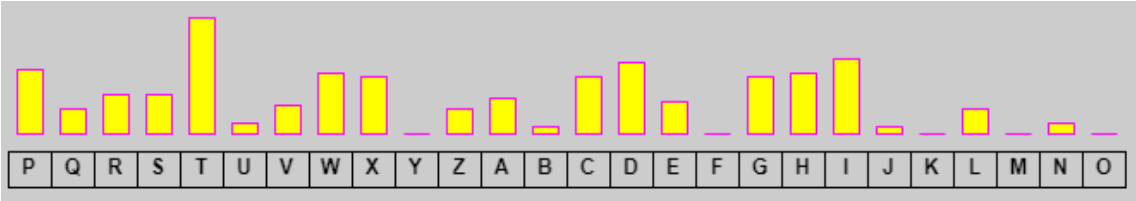


Frecvențele literelor de pe prima coloană

Testând toate cele 26 de posibile chei secrete ale unui cifru Cezar, vom obține cea mai bună potrivire în următorul caz:



Frecvențele literelor din limba engleză



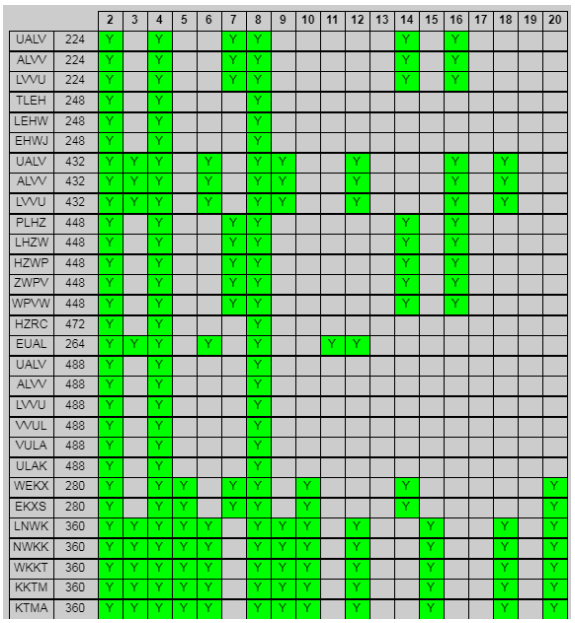
Frecvențele literelor de pe prima coloană deplasate cu 15 poziții spre dreapta

Se poate observa astfel faptul că prima literă a cheii secrete este P!

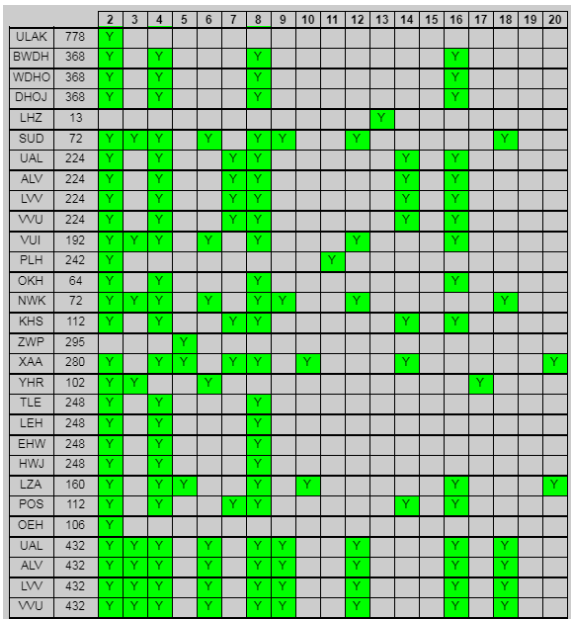
3. **Pentru a determina lungimea cheii secrete, se caută în textul cifrat grupurile repetitive formate din cel puțin 3 litere:**

IHWXEFJWLEDDZCTXBEFLARUHHCJALHZRCOXSLCCBPLHZWPVWXCUALVVULAKXKFDXAALWZ
PPOTOFTWHKLHTSSHPVUIISJKIEGPNVMOSUDBELSHQZSWEJVEGTWDSOAPQYETTOWABTLEH
WJWZGKPBWLOOCETRLAOGPVIEEGJZPVLILUDSUDAPZSXSKVPFLWNGVYTRSDSCIGHAFVOKZ
WRHWKSSIHXNVAYOKHSBQONWKLCGLZAZVWIEJGBHYHROJJAGGRCDAFCOCSWATWPWEWWEUA
LVVUIEPLHOKHGIFBKVRQCEKLNWKKTMAMOWEKXSOGNYGRAIYJWDYLPIFNABKHSTZWPOSXA
AJWYHRDRRALEQRORQEHKBVQIOXLDSMLVEFWNSTLEHWJPVVWGILZAAZXHCAHDSIKDWWNAF
FQAYHJKJZGTDSHNCXUTSKARSILVIVSJRGUTDAUPOSOTSQKPSDIDRKOEHTKXNYTAHNHTNU
ALVVUPLHZWPVWHCALWHZRCNWWZSUZWALAOBFZZNGOJOJWWENACSEHGEUALVVULAKGNWXL
CADDURVVRRATARSBVIGNWBSDITAKPOSHALSKKWEKXSTGKYCDRIXJWRVOHIYYECMDCBSLP
WJWPBWDHOJRWETMEZKXEOFLDSKDQUDSNSTWPOXLNWKKTMAMOPLWPDVWZOIHEESLEBXFDU
FLAFJLVNSCAMKRHWALYVTLEHWJWZGKPBWLOSMHGYDWPHVULHWJAOJDABWJPWRQSTJAPVV
PXUKMOSUDUIPWZDRWIEJFKTJXQSLAPIKLDNKTAZCDHOKKYVVPTMWSJHKKTPSLPSIQDFKM
XGKLIULAKBJFDUDVXSVDHIDQYVRQVEVKEAGONBQKAZVFIIFYWBVZZEQCAMJZTRWLUDZFP
LDQOWEJAEOGNRJRGSZGNHGKGAKWOYERLNLGXCKKEAJLESJLCAVNWBTHDRLJWBJPXTLWZC
LWDFTSJRRODNYOEHYWWEEWOGRJTBWDHOJRHMWLDCUWWUKJAELLGEVKPFFQVSWUQFZWNFG
JKBCBINSPSTRCVWJOOKLDNTWHZRVDSKQOHVPLAKUKBJLSEJSXZPPDRWKAQLUTCALWHZRC
NSQHFNTYUALVVUQEXGNSKKTCGM.....

4. Se calculează distanțele dintre grupurile repetitive, precum și divizorii acestora:



		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
UALV	224	Y		Y			Y	Y						Y		Y				
ALVV	224	Y		Y			Y	Y						Y		Y				
LVVU	224	Y		Y			Y	Y						Y		Y				
TLEH	248	Y		Y				Y												
LEHW	248	Y		Y				Y												
EHWJ	248	Y		Y				Y												
UALV	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
ALVV	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
LVVU	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
PLHZ	448	Y		Y			Y	Y						Y		Y				
LHZW	448	Y		Y			Y	Y						Y		Y				
HZWP	448	Y		Y			Y	Y						Y		Y				
ZWPV	448	Y		Y			Y	Y						Y		Y				
WPVW	448	Y		Y			Y	Y						Y		Y				
HZRC	472	Y		Y				Y												
EUAL	264	Y	Y	Y		Y		Y			Y	Y								
UALV	488	Y		Y				Y												
ALVV	488	Y		Y				Y												
LVVU	488	Y		Y				Y												
VVUL	488	Y		Y				Y												
VULA	488	Y		Y				Y												
ULAK	488	Y		Y				Y												
WEKX	280	Y		Y	Y		Y	Y		Y				Y						Y
EKXS	280	Y		Y	Y		Y	Y		Y				Y						Y
LNWK	360	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y			Y		Y
NWKK	360	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y			Y		Y
WKKT	360	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y			Y		Y
KKTM	360	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y			Y		Y
KTMA	360	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y			Y		Y



		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ULAK	778	Y																		
BWDH	368	Y		Y				Y								Y				
WDHO	368	Y		Y				Y								Y				
DHOJ	368	Y		Y				Y								Y				
LHZ	13												Y							
SUD	72	Y	Y	Y		Y		Y	Y			Y						Y		
UAL	224	Y		Y			Y	Y						Y		Y				
ALV	224	Y		Y			Y	Y						Y		Y				
LVV	224	Y		Y			Y	Y						Y		Y				
VVU	224	Y		Y			Y	Y						Y		Y				
VUI	192	Y	Y	Y		Y		Y				Y				Y				
PLH	242	Y									Y									
OKH	64	Y		Y				Y								Y				
NWK	72	Y	Y	Y		Y		Y	Y			Y						Y		
KHS	112	Y		Y			Y	Y						Y		Y				
ZWP	295				Y															
XAA	280	Y		Y	Y		Y	Y		Y				Y						Y
YHR	102	Y	Y			Y											Y			
TLE	248	Y		Y				Y												
LEH	248	Y		Y				Y												
EHW	248	Y		Y				Y												
HWJ	248	Y		Y				Y												
LZA	160	Y		Y	Y			Y		Y						Y				Y
POS	112	Y		Y			Y	Y						Y		Y				
OEH	106	Y																		
UAL	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
ALV	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
LVV	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		
VVU	432	Y	Y	Y		Y		Y	Y			Y				Y		Y		

Lungimea cheii secrete este divizorul care apare cel mai des!

PRINCIPIILE CRIPTOGRAFIEI MODERNE

- **Auguste Kerckhoffs** – ***La Cryptographie Militaire*** **(1883)**

1. Sistemul trebuie să fie practic, dacă nu matematic, imposibil de spart.
2. **Principiul lui Kerckhoffs:** Sistemul nu trebuie să fie secret, deoarece poate să cadă oricând în mâinile inamicului (i.e., securitatea unui sistem de criptare constă doar în menținerea secretă a cheii).
3. Cheia trebuie să fie comunicată și menținută fără a fi notată, iar utilizatorii o pot schimba sau modifica oricând doresc.
4. Sistemul trebuie să fie compatibil cu comunicarea telegrafică.
5. Sistemul trebuie să fie portabil și să nu necesite mai mult de un operator.
6. Având în vedere circumstanțele în care este utilizat, sistemul trebuie să fie ușor de utilizat, fără să necesite aplicarea multor reguli.

- https://en.wikipedia.org/wiki/Auguste_Kerckhoffs
- https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle
- http://ruxandraolimid.weebly.com/uploads/2/0/1/0/20109229/crypto_c1.pdf

- **Claude Shannon – *A Mathematical Theory of Cryptography* (1945)**

1. **Reformularea principiului lui Kerckhoffs**: "The enemy knows the system!"

2. **CONFUZIE**: orice caracter din textul cifrat depinde de cât mai multe caractere din cheia secretă pentru a ascunde corelațiile dintre ele

3. **DIFUZIE:** structura statistică a mesajului clar trebuie să fie ascunsă/disipată în mesajul criptat

- https://en.wikipedia.org/wiki/Confusion_and_diffusion
- https://www.iacr.org/museum/shannon/shannon45.pdf
- https://blogs.scientificamerican.com/cross-check/profile-of-claude-shannon-inventor-of-information-theory/