Lucrare de laborator nr. 1

1.1. Cifrul lui *Cesar*

Cifrul lui *Cesar* (sau *Cezar*). În acest cifru fiecare literă a textului clar este înlocuită cu o nouă literă obţinută printr-o deplasare alfabetică. Cheia secretă *k*, care este aceeaşi la criptare cât şi la decriptare, constă în numărul care indică deplasarea alfabetică, adică $k \in \{1, 2, 3, \ldots, n-1\}$, unde *n* este lungimea alfabetului. Criptarea şi decriptarea mesajului cu cifrul Cezar poate fi definită de formulele

$$c = e_k(x) = x + k \pmod{n},$$

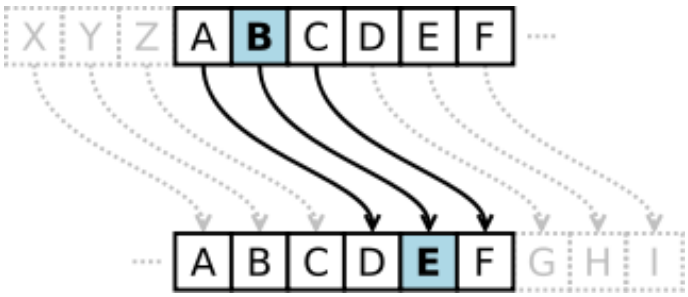
$$m = d_k(y) = y - k \pmod{n},$$

unde *x* și *y* sunt reprezentarea numerică a caracterului respectiv din textul clar *m* și din criptograma *c*. Funcţia numită *Modulo* (*a* mod *b*) returnează restul împărţirii numărului întreg *a* la numărul întreg *b*. Această metodă de criptare este numită aşa după Iulius Cezar, care o folosea pentru a comunica cu generalii săi, folosind cheia $k = 3$ (tabelul 1).

De exemplu, pentru $k = 3$ avem

$$e_k(\text{S}) = 18 + 3 \pmod{26} = 21 = \text{V},$$

$$d_k(\text{V}) = 21 - 3 \pmod{26} = 18 = \text{S},$$



În acest caz pentru *m* =„*cifrul cezar*”, obținem *c* =„*fliuxo fhcdu*”.

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
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
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
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*

Tabelul 1. *Cifrul Cezar cu cheia k*=3

Cifrul lui Cezar este foarte uşor de spart, deci este un cifru foarte slab. Astfel, un criptanalist poate obţine textul clar prin încercarea tuturor celor 25 de chei. Nu se ştie cât de util era cifrul Cezar

în timpul când era folosit de către cel de la care îi provine numele, dar este probabil ca el să fi fost destul de sigur, atât timp cât numai câţiva dintre inamicii lui Cezar erau în stare să scrie şi să citească, dar mai ales să cunoască concepte de criptanaliză.

Sarcina 1.1. **De implementat algoritmul Cezar pentru alfabetul limbii engleze în unul din limbajele de programare. Utilizați doar codificarea literelor cum este arătat în tabelul 1 (nu se permite de folosit codificările specificate în limbajul de programare, de ex. ASCII sau Unicode). Valorile cheii vor fi cuprinse între 1 și 25 inclusiv și nu se permit alte valori. Valorile caracterelor textului sunt cuprinse între 'A' și 'Z', 'a' și 'z' și nu sunt premise alte valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect. Înainte de criptare textul va fi transformat în majuscule și vor fi eliminate spațiile. Utilizatorul va putea alege operația - *criptare* sau *decriptare*, va putea introduce *cheia*, *mesajul* sau *criptograma* și va obține respectiv *criptograma* sau *mesajul decriptat*.**

1.2. Cifrul lui *Cesar* + permutare

Având în vedere criptorezistența scăzută a cifrului Cezar, datorată în primul rând spațiului de chei, care constă doar din 25 de chei diferite pentru alfabetul latin, acesta poate fi spart prin încercarea consecutivă a tuturor cheilor. Dacă mesajul a fost criptat cu cifrul Cezar, atunci una dintre chei ne va da un text citibil în limba în care a fost scris mesajul.

Spre exemplu, dacă

$$m = \texttt{BRUTE FORCE ATTACK}$$

este un mesaj scris în limba engleză și a fost criptae cu cheia

$$k = 17,$$

obținem criptograma

$$c = \texttt{SILKVWFITVRKKRTB}$$

Dacă criptanalistul interceptează mesajul criptat și parcurge toate cheile 1, 2, ..., 25 – va obține următoarele:

1	RHKJUVEHSUQJJQSA
2	QGJITUDGRTPIIPRZ
3	PFIHSTCFQSOHHOQY
4	OEHGRSBEPRNGGNPX
5	NDGFQRADOQMFFMOW
6	MCFEPQZCNPLEELNV
7	LBEDOPYBMOKDDKMU
8	KADCNOXALNJCCJLT
9	JZCBMNWZKMIBBIKS

10	IYBALMVYJLHAAHJR
11	HXAZKLUXIKGZZGIQ
12	GWZYJKTWHJFYYFHP
13	FVYXIJSVGIEXXEGO
14	EUXWHIRUFHDWWDFN
15	DTWVGHQTEGCVVCEM
16	CSVUFGPSDFBUUBDL
17	**BRUTEFORCEATTACK**
18	AQTSDENQBDZSSZBJ
19	ZPSRCDMPACYRRYAI
20	YORQBCLOZBXQQXZH
21	XNQPABKNYAWPPWYG
22	WMPOZAJMXZVOOVXF
23	VLONYZILWYUNNUWE
24	UKNMXYHKVXTMMTVD
25	TJMLWXGJUWSLLSUC

După cum se poate observa – doar textul obținut prin utiliza cheii k=17 este unul cu sens în limba engleză, deci mesajul corespunzător criptogramei este

m = BRUTEFORCEATTACK.

Pentru a spori criptorezistența cifrului Cezar se poate de aplicat o permutare a alfabetului prin aplicarea unui cuvânt-cheie (a nu se confunda cu cheia de bază a cifrului). Această cheie poate fi orice consecutivitate de litere a alfabetului - fie un cuvânt din vocabular, fie unul fără sens.

Fie cheia a doua este k_2=***cryptography***. Aplicăm această cheie asupra alfabetului

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

și obținem:

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

Această ordine nouă am obținut-o prin plasarea literelor lui k_2 la început, apoi urmează celelalte litere ale alfabetului în ordinea lor naturală. Vom ține cont de faptul că literele nu se vor repeta, adică dacă litera se întâlnește de câteva ori, ea se plasează doar o singură dată.

În continuare se aplică cifrul Cezar, ținând cont de noua ordine a alfabetului:

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

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

Tabelul 2. *Cifrul Cezar cu cheia* k_1=3 *și* k_2=*cryptography*

Deoarece există 26!= 403291461126605635584000000, numărul de chei pentru această versiune a algoritmului va fi

$$26! \cdot 25 = 10082286528165140889600000000,$$

ceea ce complică spargerea prin metoda exhaustivă, dar nu ne salvează de atacul prin analiza frecvențelor.

Sarcina 1.2. **De implementat algoritmul Cezar cu 2 chei, cu păstrarea condițiilor exprimate în Sarcina 1.1. În plus, cheia 2 trebuie să conțină doar litere ale alfabetului latin, și să aibă o lungime nu mai mică de 7.**

Sarcina 1.3. **Pentru această sarcină studenții se vor diviza în perechi. Fiecare dintre ei va cripta câte un mesaj alcătuit din 7-10 simboluri (fără spații și scris doar cu majuscule) cu versiunea cifrului *Cesar* cu permutare, alegând fiecare cheile sale. Criptogramele astfel obținute vor fi transmise colegului, împreună cu cheile respective. Fiecare dintre cei doi va realiza decriptarea și se va face compararea cu versiunea originală a colegului.**

Raportul final va fin încărcat pe ELSE în limita termenului stabilit de profesor. Fiecare săptămână de întârziere se penalizează cu câte un punct al notei de evaluare.