

CRIPTARE SIMETRICA

Lucrarea de laborator #1

Metoda substitutiei

Breviar teoretic

Operatia de cifrare se bazeaza pe o corespondenta biunivoca intre alfabetul clar, si alfabetul cifrat. Se presupune ca alfabetul clar este format din cele 26 de litere (in limba romana fara diacritice) plus delimitatorul de cuvânt spatiul. Alfabetul cifrat poate fi format din aceleasi caractere sau doar din cele 26 de litere (ale limbii romane) caz in care spatiul se va inlocui cu cea mai putin frecventa litera (Q) sau se va ignora pur si simplu. In continuare, delimitatorul de cuvânt este inlocuit cu litera Q.

Corespondenta dintre cele doua alfabete poate fi:

- aleatoare;
- pseudoaleatoare: plecand de la o parola se construiește alfabetul cifrat.

Intrucat in cazul corespondentei aleatoare lucrurile sunt cat se poate de clare, vom

prezenta pe scurt o metoda de constructie a corespondentei in cel de-al doilea caz. Pornind de la o parola, alfabetul cifrat este construit dupa urmatorul algoritm:

- se scriu, o singura data, in ordinea aparitiei, literele din parola;
- se scriu literele alfabetului care nu apar in parola.

Corespondenta între cele două alfabetice se realizează după regula alfabet în alfabet după

o permutare fixă π (aceasta poate fi chiar permutarea identică iar la descifrare se aplică același procedeu doar cu inversa permutării π).

În funcție de forma permutării substituției se numește:

- **directă** (alfabetul cifrat are același sens lexicografic cu alfabetul clar, sunt în total 26 astfel de substituții).

Exemplu de substituție directă:

A	B	C	D	E	F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N	O	P	Q	R	S

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C	D	E	F

- **inversă** (alfabetul cifrat are sens invers lexicografic cu alfabetul clar, sunt în total 26 de astfel de substituții).

Exemplu de substituție inversă:

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

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

Definiție Un cifru de substituție este liniar de la Z_m la Z_m (m fiind numărul de caractere al alfabetului sursă) dacă poate fi descris prin funcția $f : Z_m \rightarrow Z_m$ definită prin $f(x) = ax + b$ cu $\gcd(a, m) = 1$, funcția de descifrare fiind $f^{-1}(x) = a^{-1}(x - b)$. Cheia de cifrare o formează numerele a și b .

Exemple de exercitii de criptare și decriptare

rezolvate

Exercitiul 1 Sa se construiasca alfabetul de cifrare cu ajutorul parolei

TESTARE SISTEM

iar apoi sa se cifreze mesajul

IN CRIPTOGRAFIE NICI O REGULA NU ESTE ABSOLUTA.

Permutarea care realizeaza corespondenta este:

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

Rezolvare

Corespondenta dintre alfabetul clar si alfabetul de cifrare (inainte de realizarea permutarii) este:

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

Corespondenta dintre alfabetul clar si alfabetul de cifrare dupa realizarea permutarii este:

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

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

Mesajul clar se proceseaza astfel incat spatiul(simbolul) este inlocuit cu cea mai putin frecventa litera - Q din limba vorbita:

INQCRIPTOGRAFIEQNICIQOQREGULAQNUQESTEQAABSOLU
TA.

Mesajul cifrat va fi:

OHDXC OFMGQ CZUOV DHOXO DGDCV QIKZD HIDVB
MVDZY BGKIM Z.

Exercitiul 2 Sa se descifreze mesajul:

DOJMD OVPGF OMATN BXXXX

algoritmul utilizat fiind o substitutie simpla, determinata de cuvantul
cheie

PASSWORD.

Rezolvare:

Correspondenta dintre alfabetul clar si alfabetul de cifrare este:

A	B	C	D	E	F	G	H	I	J	K	L	M
P	A	S	W	O	R	D	B	C	E	F	G	H

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	J	K	L	M	N	Q	T	U	V	X	Y	Z

Analizati exemple de programe de criptare

CRIPTARE CU SUBSTITUIRE

```
// Program de criptare cu substitutie

// programul a fost implementat doar pentru majuscule

// fara semne de punctuatie

#include <stdio.h>

#include <conio.h>

#include <stdlib.h>

char Cheie[]="DIFKOZWQJANMLHEGVTSRPBCYXU";

// Functia de criptare

char * Criptare(char * textC)

{

int i;;

char rez[100];;

rez[0]='\0';; for(i=0;;i<strlen(textC);;i++)

rez[i]=Cheie[textC[i]%65];; rez[i]='\0';;

return rez;;
```

```

}

// Determinarea pozitiei in cheie a caracterului

// necesara refacerii corespondentei initiale

// identica alfabetului

int Pozitia(char *Cheia, char ch)

{
int i=0,poz=-1;; while(poz==-1)
{

if(Cheia[i]==ch)
poz=i;

else
i++;

}
return poz;

}

// Functia de Decriptare

char * Decriptare(char * textC) {

int i,poz;;
char rez[100];
rez[0]='\0';

for(i=0;;i<strlen(textC);i++)

    rez[i]=Pozitia(Cheie,textC[i])+65;

return rez;;

}

void main()

```

```

{
char textClar[101]="ACESTAESTETEXTULDECRIPATAT";

char textCifrat[101],textDecript[101];
clrscr();
strcpy(textCifrat, Criptare(textClar));

strcpy(textDecript,Decriptare(textCifrat));

printf("\nTextul in clar este :\\t\\t%s\\n",textClar);

printf("\nTextul codificat este :\\t\\t%s\\n",textCifrat);

printf("\nTextul decodificat este :\\t%s\\n",textDecript);;

}

```

CRIPTARE CU SUBSTITUIRE CU GENERAREA CHEII DE CRIPTARE

```

// Program de cripare cu substitutie

// programul a fost implementat doar pentru majuscule
// fara semne de punctuatie
// iar cheia este generata dupa o anumita secventa numerica secreta

#include <stdio.h>

#include <conio.h>

#include <stdlib.h>

char Cheie[27]; // cheia ce se va genera
int numCheie[8]={3,4,8,7,5,1,6,2};; // secventa secreta
char matr[4][9];; // matricea in care se stocheaza intermediar cheia
secreta

char * GenerezCheie(int CheieSecreta[8])

{

```

```

int i,j,k=0,caut=1,poz,indice=0;; char rez[27];;
rez[0]='\0';;
for(i=0;;i<4;;i++)

{

    for(j=0;;j<8;;j++)

    matr[i][j]='A'+k++;; matr[i][j]='\0';;

}

for(k=0;;k<8;;k++)

{
    poz=0;

    while(CheieSecreta[poz]!=caut)

    poz++;

    for(i=0;;i<4;;i++)

    {
        if((i<3)|| (i==3 && poz<2))

        rez[indice++]=matr[i][poz];

    }

    caut++;

}

rez[indice]='\0';

return rez;;

}

```

// Functia de criptare


```

char * Criptare(char * textC)
{
    int i;
    char rez[100];
    rez[0]='\0';

    for(i=0;i<strlen(textC);i++)
        rez[i]=Cheie[textC[i]%65];; rez[i]='\0';

    return rez;
}

// Determinarea pozitiei in cheie a caracterului
int Pozitia(char *Cheia, char ch)
{
    int i=0,poz=-1;

    while(poz==-1)
    {
        if(Cheia[i]==ch)
            poz=i;
        else
            i++;
    }

    return poz;
}

// Functia de Decriptare

```

```

char * Decriptare(char * textC)
{
    int i,poz;
    char rez[100];
    rez[0]='\0'; for(i=0;;i<strlen(textC);i++)

    rez[i]=Pozitia(Cheie,textC[i])+65;

    return rez;;
}

void main()
{
    char textClar[101]="ACESTAESTETEXTULDECRIPATAT";

    char textCifrat[101],textDecript[101];
    Cheie[0]='\0';
    strcpy(Cheie,GenerezCheie(numCheie));

    clrscr();
    strcpy(textCifrat, Criptare(textClar));

    strcpy(textDecript,Decriptare(textCifrat));

    printf("\nTextul in clar este :%s\n",textClar);;
    printf("\nTextul codificat este :%s\n",textCifrat);
    printf("\nTextul decodificat este :%s\n",textDecript);
}

```

Compuneti propriul program de criptare-decriptare ,care utilizeaza metoda substitutiei .

