Tehnici de criptanaliza

Student: Muresan Malvina Narcisa

Cuprins

1. Obiectul criptanalizei
2. Resursele necesare de calcul
3. Substitutia simpla
4. Substitutia multipla
5. Identificarea cifrului de substitutie poligrafica
6. Cifrul Playfair
7. Substitutia polialfabetica
8. Solutia unui cifru de substitutie
9. Transpozitia

10. Sisteme mixte

11. Proceduri de identificare a sistemului

12. Concluzii

13. Aplicatii

1. **Obiectul criptanalizei**

**Criptanaliza** este studiul metodelor de obținere a înțelesului informațiilor criptate, fără a avea acces la informația secretă necesară în mod normal pentru aceasta. De regulă, aceasta implică găsirea unei chei secrete. Într-un limbaj non-tehnic, aceasta este practica **spargerii codurilor**.

Termenul de criptanaliză este folosit și cu referire la orice încercare de a ocoli mecanismele de securitate ale diferitelor tipuri de protocoale și algoritmi criptografici în general, și nu doar al criptării informației. Totuși, criptanaliza de regulă exclude metode de atac care nu țintesc slăbiciunile conceptuale ale [criptografiei](https://ro.wikipedia.org/wiki/Criptografie), cum ar fi [mita](https://ro.wikipedia.org/w/index.php?title=Mita&action=edit&redlink=1), extragerea informațiilor prin constrângeri fizice, intrarea prin efracție, logarea tastelor apăsate, și social engineering, deși aceste tipuri de atac sunt o problemă importantă și sunt adesea mai eficiente decât criptanaliza tradițională.

Deși scopul a rămas același, tehnicile și metodele de criptanaliză s-au schimbat drastic de-a lungul istoriei criptografiei, adaptându-se la creșterea complexității criptografice, de la metodele cu creionul și hârtia din trecut la mașini ca [Enigma](https://ro.wikipedia.org/wiki/Ma%C8%99ina_Enigma) din [al doilea război mondial](https://ro.wikipedia.org/wiki/Al_doilea_r%C4%83zboi_mondial), până la schemele criptografice computerizate din

zilele noastre. Rezultatele criptanalizei au variat și ele—nu mai este posibil să se obțină succese nelimitate în spargerea codurilor și există o clasificare ierarhică a ceea ce constituie un atac practic. La jumătatea anilor 1970, s-a introdus o nouă clasă criptografică:criptografia asimetrică. Metodele de spargere a acestor criptosisteme sunt radical diferite de cele anterioare, și implică de regulă rezolvarea unor probleme construite cu grijă în matematică, cea mai celebră dintre acestea fiind [factorizarea întregilor](https://ro.wikipedia.org/wiki/Factorizarea_%C3%AEntregilor).

Având în vedere unele date criptate ("textul cifrat"), scopul criptanalizatorului este de a obține cât mai multe [informații](https://ro.wikipedia.org/wiki/Informa%C8%9Bie) posibile despre datele originale, necriptate ("textul clar"). Este util să se ia în considerare două aspecte ale realizării acestui obiectiv. Primul este ruperea sistemului - care este descoperirea modului în care funcționează procesul de encirculare. Al doilea este rezolvarea cheii care este unică pentru un anumit mesaj criptat sau pentru un grup de mesaje.

### Resursele necesare de calcul

Atacurile pot fi, de asemenea, caracterizate de resursele de care au nevoie. Aceste resurse includ:

* *Timp* - numărul de etape de calcul (de exemplu, criptări de testare) care trebuie efectuate.
* *Memorie* - cantitatea de spațiu de stocare necesară pentru efectuarea atacului.
* *Date* - cantitatea și tipul textelor libere și textului cifrat necesare unei anumite abordări.

Este uneori dificilă prezicerea exactă a acestor cantități, mai ales atunci când atacul nu este practic de implementat pentru testare. Dar criptanaliștii academici tind să furnizeze cel puțin ordinea estimată de amploare a dificultăților atacurilor lor, spunând, de exemplu, "coliziunile SHA-1 acum 252.[[1]](https://ro.wikipedia.org/wiki/Criptanaliz%C4%83#cite_note-1)

[Bruce Schneier](https://ro.wikipedia.org/wiki/Bruce_Schneier) observă că și atacurile nepractice, computațional pot fi considerate pauze: "Ruperea unui cifru înseamnă pur și simplu găsirea unei slăbiciuni în cifrul care poate fi exploatată cu o complexitate mai mică decât forța bruta. Nu contează că forța brută ar putea necesita criptare de 2128; un atac care necesită 2110 de criptare ar fi considerat o pauză, ce poate fi doar o slăbiciune certificată: dovezi că cifrul nu funcționează ca publicitate.[[2]](https://ro.wikipedia.org/wiki/Criptanaliz%C4%83#cite_note-schneier-2)

1. [**^**](https://ro.wikipedia.org/wiki/Criptanaliz%C4%83#cite_ref-1) *McDonald, Cameron; Hawkes, Philip;* [*Pieprzyk, Josef*](https://ro.wikipedia.org/w/index.php?title=Josef_Pieprzyk&action=edit&redlink=1)*,* [*SHA-1 collisions now 252*](http://eurocrypt2009rump.cr.yp.to/837a0a8086fa6ca714249409ddfae43d.pdf) *(PDF), accesat în 4 aprilie 2012*
2. [**^**](https://ro.wikipedia.org/wiki/Criptanaliz%C4%83#cite_ref-schneier_2-0) [Schneier 2000](https://ro.wikipedia.org/wiki/Criptanaliz%C4%83#CITEREFSchneier2000).
3. **Substitutia simpla**

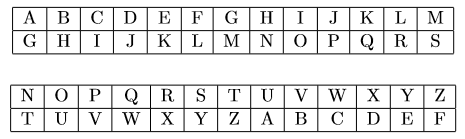
Operatia de cifrare se bazeaza pe o corespondenta biunivoca intre alfabetul clar notat prin A si alfabetul cifrat notat prin C. Pentru exempliﬁcarea ideilor vom prezupune ca alfabetul clar este format din cele 26 de litere ale limbii romane (fara diacritice) plus delimitatorul de cuvant spatiul. Alfabetul cifrat poate ﬁ format din aceeleasi caractere sau doar din cele 26 de litere ale limbii romane cazin care spatiul se vainlocui cu cea mai putin frecventa litera (Q) sau se va ignora pur si simplu. Corespondenta dintre cele doua alfabete (presupunem ca delimitatorul de cuvant esteinlocuit cu litera Q) poate ﬁ: -aleatoare; -pseudoaleatoare: plecand de la o parola se construieste alfabetul cifrat. Dacain 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;

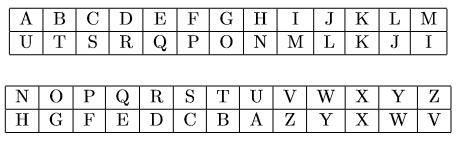
-se scriu literele alfabetului ce nu aparin parola.

Corespondenta intre cele doua alfabete se realizeaza dupa regula alfabetin alfabet dupa o permutare ﬁxa σ (aceasta poate ﬁ chiar permutarea identica iar la decriptare se aplica aceelasi procedeu dar cu inversa permutarii σ). In functie de forma permutarii substitutia se numeste:

-directa (alfabetul cifrat are acelasi sens lexicograﬁc cu alfabetul clar, sunt in total 26 astfel de substitutii). Exemplu de substitutie directa:

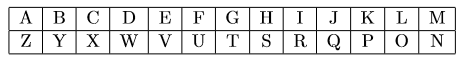


-inversa (alfabetul cifrat are sens invers lexicograﬁc cu alfabetul clar, suntin total 26 de astfel de substitutii). Exemplu de substitutie inversa:

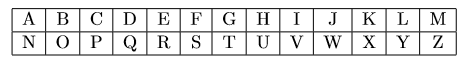


Reamintim aici trei exemple celebre (vechile codurie braice) de substitutii reciproce (daca litera X se substituie cu litera Y atunci Y se va substitui cu X) si anume:

-atbash (prima jumatate a literelor alfabetului se mapeaza in cea de-a doua jumatatein ordine invers lexicograﬁca):



-albam(prima jumatate a literelor alfabetului semapeaza inceade-adouajumatate in ordine lexicograﬁca):



-atbah:



Deﬁnitia 1. Un cifru de substitutie liniar de la Zm la Zm (m ﬁind numarul de caractere al alfabetului sursa) poate ﬁ descris prin functia f : Zm →Zm deﬁnita prin f(x) = αx+β cu gcd(α,m) = 1, functia de descifrare ﬁind f−1(x) = α−1(x−β). Cheia de cifrare sunt numerele α si β.

Observatia 1. Primul manual de analiza criptograﬁca a cifrurilor de substitutie a fost scris de Al-Kindi [2]in anul 850 AD.

Observatia 2. Cifrul de substitutie are proprietatea de confuzie (ascunderea legaturii dintre textul clar si textul cifrat).

1. **Substitutia multipla**

In cazul substitutiei multiple (substitutie poligraﬁca) M caractere din textul clar sunt substituitein N caractere de text cifrat. Evident pentru ca operatia de cifrare sa ﬁe reversibila trebuie ca M ≥N. Daca M = N = 2 atunci cifrul se numeste cifru de substitutie digraﬁca.

Deﬁnitia 1 Un cifru de substitutie poligraﬁca liniar de la Zk m la Zk m (m ﬁind numarul de caractere al alfabetului sursa si k dimensiunea k−gramei) poate ﬁ descris prin functia f : Zk m → Zk m deﬁnita prin f(x) = Ax + β cu matricea A inversabila, functia de descifrare ﬁind f−1(y) = A−1(y−β). Cheia de cifrare este matricea A si vectorul β.

1. **Identiﬁcarea cifrului de substitutie poligraﬁca**

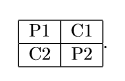
Un cifru de substitutie poligraﬁca se poate detecta foarte usor dupa frecventa N−gramelor. Distributia acestora este departe de a ﬁ uniforma. Evident, o conditie necesara de identiﬁcare a acestui tip de cifru este aceea ca dimensiunea mesajului cifrat sa ﬁe suﬁcient de mare. O procedura de detectare a lui N se bazeaza, de exemplu, pe minimul entropei H calculate din R−grame:

H (m;N) = min R H (m;R).

Alteprocedurideidentiﬁcarecorectaaparametruluinsuntprezentateinsectiunea Proceduri de identiﬁcare a sistemului. Pentru a se asigura biunivocitatea parametrul M trebuie sa ﬁe egal cu N. Constructia tabelei de substitutie poligraﬁca se realizeaza cu ajutorul frecventei N−gramelor din textul cifrat.

1. **Cifrul celor 4(2) tabele rectangulare**

In continuare vom prezenta doua sisteme de cifrare de tip substitutie digraﬁca. Literele alfabetelor (clar si cifrat) sunt trecute intr-un careu de 5×5 (litera I ﬁind asimilata literei J). Modul de aranjare al literelor alfabetelor clar este ﬁxat apriori (de exemplu ordine lexico graﬁca)iar alalfabetelor cifrate in functie de parola. Textul clar este preprocesat astfel incat acesta sa ﬁe compatibil cu matricea de cifrare (delimitatorul de cuvant este ignorat sau este inlocuit cu cea mai putin frecventa litera, litera I este asimilata cu litera J, si in ﬁne daca este cazul mai adjunctionam o litera la text pentru a avea un numar par de digrame). Pentru cifrul celor 4 tabele regula de cifrare este data de regula dreptunghiului: o digrama din textul clar se cifreaza in digrama corespunzatoare diagonalei secundare a dreptunghiului determinat de cele doua caractere ale digramei clare. Modul de aranjare al celor patru alfabete (P1 si P2 sunt alfabetele clare iar C1 si C2 sunt alfabetele cifratein functie de parola) este prezentat mai jos:



Algoritmul prezentat mai sus degenereazain algoritmul celor doua tabele (verticale sau orizontale) dupa cum urmeaza: P1 ≡ C1 si P2 ≡ C2 respectiv P1 ≡ C2 si P2≡C1. Daca literele ce formeaza digrama se aﬂa pe aceeasi coloana, respectiv linie, atunci reprezentarea cifrata a acestora sunt eleinsele, respectiv acestea scrise in ordine inversa. Cele doua tabele de cifrare sunt:



respectiv



1. **Cifrul Playfair**

Cifrul Playfair (numele acestui sistem de cifrare provine de la Lordul englez Playfair) este unul dintre cele mai cunoscute sisteme de cifrare digraﬁce (transforma un grup de 2 litereintr-un grup de alte doua litere). Acest sistem de cifrare este foarte simplu de folosit dar mult mai sigur decat sistemele de substitutie monoalfabetice. Descriemin continuare modul de utilizare al acestui sistem de cifrare. Literele alfabetului sunt trecuteintr-un careu de 5×5 (litera I ﬁind asimilata literei J). Textul clar este preprocesat astfelincat acesta sa ﬁe compatibil cu matricea de cifrare (delimitatorul de cuvant este ignorat sau esteinlocuit cu cea mai putin frecventa litera, litera I este asimilata cu litera J, siin ﬁne daca este cazul mai adjunctionam o litera la text pentru a avea un numar par de digrame).

Regula de cifrare este urmatoarea:

1. Daca digrama ce se doreste cifrata nu are literele pe aceeiasi linie sau coloana, atunci regula de cifrare este regula dreptunghiului, traseul ﬁind pe verticala de la cea de-a doua litera a digramei catre prima litera.
2. Daca digrama ce se doreste cifrata are literele pe aceeiasi linie, atunci se aplica regula: cifreaza la dreapta, descifreaza la stanga.
3. Daca digrama ce se doreste cifrata are literele pe aceeiasi coloana, atunci se aplica regula: cifreaza in jos, descifreaza in sus.

Observatia 1. Daca o digrama aparein textul clarin ordine inversa atunci acelasi lucru se vaintampla siin textul cifrat.

Observatia 2 Cifrul Playfair nu are regula pentru cifrarea literelor duble: digramele ce contin doua litere identice sunt sparte prin introducerea artiﬁciala a unei alte litere.

Observatia 3 Cifrul Playfair apare ca o extindere, in sensul reducerii numarului de tabele rectangulare folosite (de la doua la unul), al cifrului cu 2 tabele.

Metoda cea mai freventa de atac a acestui tip de cifru constain analiza frecventei digramelor de text clar combinata cu metoda comparatiei patternurilor din textul cifrat cu patternuri din dictionar. SpectaculosestefaptulcainManualul Teroristului [104],in capitolul 13 intitulat Scrieri Secrete, Coduri si Cifruri, se prezinta tehnici steganograﬁce, tehnici de codiﬁcare si o serie de metode de cifrare clasice cum ar ﬁ substitutia simpla si substitutia multipla.­

**8. Substitutia polialfabetica**

Caracteristicile si identiﬁcarea sistemelor de substitutie polialfabetica

Un sistem de cifrare de tip substitutie polialfabetica este generalizarea sistemului de cifrare de substitutie monoalfabetica. Fie un sistem de cifrare polialfabetic compus dintr-un numar N de alfabete. Fiecare alfabet reprezinta o permutare (stabilita in functie de parola) a alfabetului de intrare. Algoritmul de cifrare consta in substituirea celei de a i−a litere m din textul clar cu litera corespunzatoare din cel de al imodN alfabet. Sistemele polialfabetice sunt usor de identiﬁcat prin aplicarea tehnicii frecventelor secventelor decimate din textul cifrat sau a valorii maxime a functiei Kappa (v. paragraful Proceduri de identiﬁcare a sistemului).

Atacul sistemelor polialfabetice Atacul sistemelor polialfabetice este similar cu atacul a N sisteme de substitutie monoalfabetica. Deci, o procedura de tip divide et impera are o compexitate de O(N). Procedura este descrisain continuare:

Intrare: Textul cifrat de lungime M suﬁcient de mare.

Iesire: Textul clar corespunzator sistemului de cifrare polialfabetic.

Pas 1. Determina numarul de alfabete N.

Pas 2. Pentru j = 0 to 4 executa: pentru i = 1 to N −j executa: aplicaproceduradereconstructiepartiala(pebazafrecventelor (j +1)−gramelor) a alfabetelor i,...,i+j.

Pas 3. Conform celor N alfabete reconstruieste textul clar.

Observatia 1. Procedura descrisa mai sus are ca parametru implicit de analiza numarul maxim de legaturi 4 : astfel, 1−gramele sunt caracterele, 2−gramele sunt dubletii, etc.

d2) reconstructia cheilor folositein operatia de cifrare; d3)reconstructiacheilorsauacuvintelorcheieceaufostfolositepentruconstructia sirurilor de alfabete.

**9. Transpozitia**

Daca substitutia schimba valoarea unui caracter din textul cifrat, permutarea schimba pozitia pe care acest caracter apare in textul cifrat si nu valoarea sa. Operatia de cifrare prin permutarea σ ∈ SN se realizeaza prin permutarea caracterelor din blocurile adiacente, de lungime N, ale textului clar. Un caz particular al permutarii este aceela al transpozitiei de lungime N. Textul este scrisintr-o tabela (completa sau nu) cu N coloane, literele ﬁind scrise linie cu linie. Pornind de la o parola literala se construieste o parola numerica (spre exemplu se asocieaza ﬁecarei litere din parola pozitia sa in scrierea lexicograﬁca a acesteia). Textul este apoi citit coloana cu coloanaintr-o ordine stabilita apriori (crescator, descrescator, etc.). Pentru descifrare se aplica acelasi algoritm dar cu parola numerica σ−1.

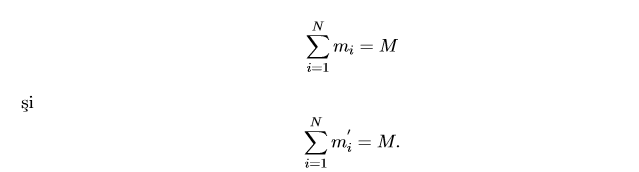
Observatia 6.4.1. Cifrul de transpozitie (mai general cifrul de permutare) are proprietatea de difuzie (disiparea redundantei textului clar de-a lungul textului cifrat).

**10. Sisteme mixte**

Sistemele mixte de cifrare au la baza o cifrare succesiva a mesajului prin metoda substitutiei iar apoi prin metoda transpozitiei sau viceversa. Tot ceea ce trebuie sa facem acum este sa atacam sistemul de cifrare de la ultima sa componenta catre prima. Remarcam faptul ca in cazul substitutiei simple aceasta este comutativa cu operatia de transpozitie deci se poate aborda maiintai substitutia iar apoi transpozitia. in cazul utilizarii unui sistem polialfabetic, cu numar necunoscut de alfabete, recomandarea este ca dupa stabilirea, prin metode statistice, a numarului de alfabete, sa se abordeze concomitent identiﬁcarea efectiva a alfabetelor si al transpozitiei utilizate. in cazul utilizarii unui sistem poligraﬁc (tabele de cifrare) si o transpozitie este recomandabila o tehnica de tip backtracking.

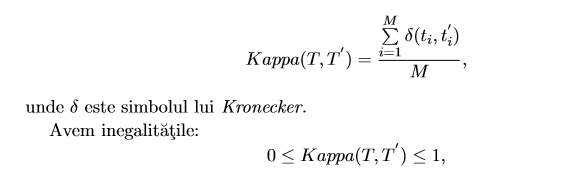
**11. Proceduri de identiﬁcare a sistemului**

Procedurile de criptanaliza prezentate in cadrul acestui paragraf sunt bazate pe calculul unor estimatori pentru o serie de functii de test (vezi Friedman [20], Bauer [6], Preda si Simion [58]). Textul clar trebuie sa ﬁe omogen din punct de vedere statistic. Daca textul nu este omogen, atunci, cu ajutorul unei proceduri, acesta se poate divizain parti omogene. Procedurile ce urmeaza ne permit sa identiﬁcam modelul de cifrare, structura statistica a textului clar si in cele din urma solutia problemei. Sa notam prin T = (t1,...,tM) si T0 = (t0 1,...,t0M) doua siruri de lungime M din acelasi vocabular ZN (de lungime N). Notam prin mi si m0 i frecventele de aparitie ale celei de a i−a litere din alfabetul sursa din sirul T respectiv T0. Avem deci:



in cele ce urmeaza vom descrie functiile de decizie Kappa, Chi, Psi si Phi.

1. Functia Kappa Functia de test Kappa este deﬁnita prin:

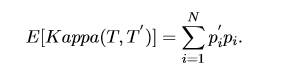


cu egalitatein partea stanga pentru ti 6= t0 i (pentru orice i) respectiv T ≡T0. Testul Kappa este similar cu testul de corelatie. Cateodata Kappa se va nota mai simplu prin K. Avem urmatoarele teoreme de invarianta (vezi Bauer [6]):

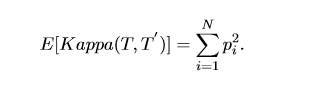
Teorema 1. Pentru toate sistemele de cifrare de tip substitutie polialfabetica valoarea lui Kappa a doua texte de lungimi egale, cifrate cu aceeasi cheie, este invarianta.

Teorema 2. Pentru toate sistemele de cifrare de tip transpozitie valoarea lui Kappa a doua texte de lungimi egale, cifrate cu aceeasi cheie, este invarianta.

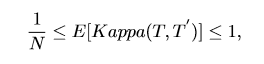
Valoarea medie a lui Kappa(T,T0), pentru T si T0 deﬁnite de doua surse Q respectiv Q0 (cu probabilitatea simbolurilor pi respectiv p0 i pentru i = = 1,...,N) este:



Daca sursele Q si Q0 sunt identice (acest lucru se noteaza prin Q ≡ Q0), adicap i = p0 i, atunci:



Teorema 3. Pentru doua surse identice Q si Q0 are loc inegalitatea:



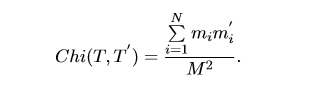
cu egalitatein partea stanga pentru distributia uniforma, iarin partea dreapta pentru sursa determinista (adica exista un indice i pentru care pi = 1).

Observatia 1. Dispersia functiei Kappa se calculeaza dupa formula:



Observatia 2. Functia Kappa poate ﬁ folosita la atacul sistemelor polialfabetice: diferenta dintre valorile maxime ale valorilor Kappa(T(i),T) (am notat prin T(i) textul T deplasat ciclic cu i pozitii la dreapta) este divizibil cu numarul de alfabete utilizate. Pentru a gasi alfabetele utilizate se poate aplica o tehnica de tip divide et impera si o procedura bazata pe maximul frecventei sau atac de tip stereotip.

2. Functia Chi Functia Chi este deﬁnita prin formula:

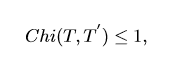


Vom nota aceasta functie si prin litera greceasca χ. Au loc urmatoarele teoreme de invarianta (vezi Bauer [6]):

Teorema 4. Pentru toate sistemele de cifrare de tip substitutie monoalfabetica valoarea lui Chi a doua texte de lungimi egale, cifrate cu aceeasi cheie, este invarianta.

Teorema 5. Pentru toate sistemele de cifrare de tip transpozitie valoarea lui Chi a doua texte de lungimi egale, cifrate cu aceeasi cheie, este invarianta.

Avem inegalitatea:



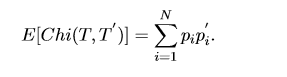
cu egalitate pentru T ≡ T0. Pentru un text cu distributie uniforma T (mi = M N

) si

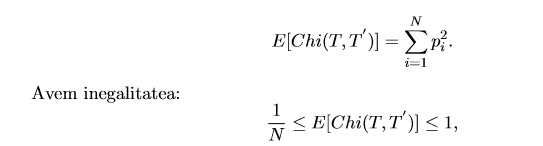
un text arbitrar T0 avem:



Valoarea medie a lui Chi a doua texte T si T0 de lungime egala M peste aceelasi vocabular ZN se calculeaza din probabilitatile pi si p0 i ale frecvetei de aparitie ale celui de al i-lea caracterin sursele stochastice Q si Q0 ale textelor:



Daca sursele Q si Q0 sunt identice atunci pi = p0 i pentru orice i si



Cu egalitate in partea stanga pentru distributia uniforma iar in partea dreapta pentru sursa determinista.

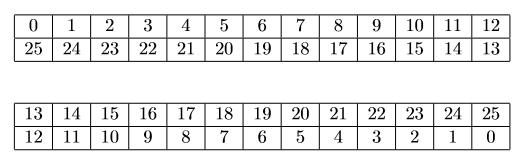
**12. Concluzii**

Functiile de test deﬁnite in cadrul acestui capitol sunt in variante in cazul folosirii anumitor sisteme de cifrare cum ar ﬁ sistemele de cifrare de tip transpozitie si de substitutie mono sau polialfabetica. Aceste functii de test pot ﬁ folosite in identiﬁcarea limbii folosite in textul clar, a sistemului de cifrare folosit, a cheii si in cele din urma a textului clar. Functia Kappa este folositain identiﬁcarea sistemului de cifrare si in identiﬁcarea limbii folosite in textul clar. Procedura de identiﬁcare a limbii se bazeaza pe compararea valorilor lui Psi si Phi ale textului cifrat cu valorile lui Psi si Phi ale ﬁecarei limbi (aceste functii de test devin in acest moment teste de conﬁrmare). Functiile Chi sunt folosite in atacuri de tip isolog (texte diferite cifrate cu aceeiasi cheie). Testele Kappa,Chi,Psi si Phi se pot efctua pe digrame sau trigrame, etc. Alte aplicatii criptograﬁce sunt cele de tip cautare inteligenta a parolelor sau de tip dictionar modiﬁcat (conform unor reguli lexicale). Cele mai bune rezultate sunt obtinute daca se analizeaza textul format numai din litere mari sau mici. Textele pot ﬁ cu delimitator de cuvant (spatiu) sau fara delimitator de cuvant. Descrierea completa a acestor tipurilor de cifruri prezentate in cadrul acestui capitol precum si principalele moduri de atac se poate gasi de exempluin Bauer [6].

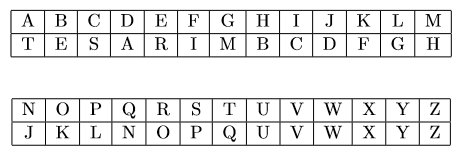
**12. Aplicatii**

Exercitiul 1. Care este diferenta dintre proprietatea de confuzie si proprietatea de difuzie a unui algoritm de cifrare?

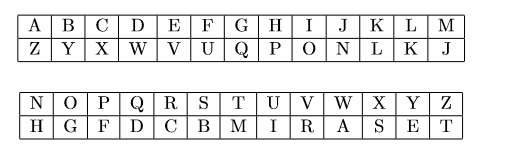
Exercitiul 2. Sa se construiasca alfabetul cifrat cu ajutorul parolei de cifrare TESTARESISTEM iar apoi sa se cifreze mesajul ”IN CRIPTOGRAFIE NICIO REGULA NU ESTE ABSOLUTA” .Permutarea ce realizeaza corespondenta este:



Raspuns. Corepondenta dintre alfabetul clar si alfabetul cifrat (inainte de realizarea permutarii) este:



Corepondenta dintre alfabetul clar si alfabetul cifrat dupa realizarea permutarii este:



Mesajul clar se proceseaza astfel incat spatiul este inlocuit cu cea mai putin frecventa litera:

INQCRIPTOGRAFIEQNICIQREGULAQNUQESTEQABSOLUTA.

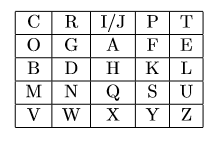
Mesajul cifrat va ﬁ:

OHDXCOFMGQCZUOV DHOXODCV QIKZDHIDV BMV DZY BGKIMZ.

Exercitiul 3. Sa se cifreze mesajul ”SI IN CRIPTOGRAFIE TACEREA ESTE AUR” cu ajutorul metodei celor 4 tabele initializate cu parolele de cifrare CRIPTOGRAFIE si TEST.

Exercitiul 4. Sa se construiasca matricea de cifrare Playfair cu ajutorul parolei CRIPTOGRAFIE iar apoi sa se cifreze mesajul ”SI IN CRIPTOGRAFIE TACEREA ESTE AUR”.

Raspuns. Matricea Playfair se obtine trecand literele din parola o singura data in careul de 5×5, iar apoi celelalte litere ale alfabetuluiin ordinea lexicograﬁca:



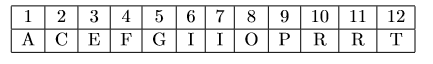
Mesajul este preprocesat prin introducerea literei Q ca delimitator de cuvant, adjunctionandu-se la ﬁnalul mesajului (pentru ca acesta sa aiba lungime para) litera Q: SIQINQCRIPTOGRAFIEQTACEREAQESTEQAURQ.

Respectand regulile de cifrare Playfair mesajul cifrat devine:

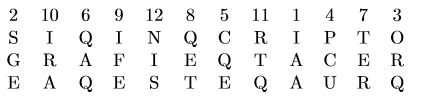
QPXAQSRIPTCEDGFETAUIOIGTOFUAUPAUEQIN.

Exercitiul 5. Sa se cifreze prin metoda transpozitiei (N = 12), pornind de la parola CRIPTOGRAFIE mesajul ”SI IN CRIPTOGRAFIE TACEREA ESTE AUR”.

Raspuns. Vom construi secventa numerica de cifrare asociind ﬁecarei litere din parola indicele din ordinea lexicograﬁca: astfel literele din parola, scrise in ordine lexicograﬁca sunt:



deci parola CRIPTOGRAFIE produce permutarea: 2 10 6 9 12 8 5 11 1 4 7 3. Textul clar este scrisintr-o tabela cu 12 coloane:



Deoarece lungimea textului nu este divizibila cu 12 vom completa ultimul rand cu o secventa cunoscuta (in acest caz caracterul Q). Textul cifrat se obtine citind coloanele tabelei de cifrarein ordinea indicata de parola numerica:

IAASGEORRQPCUCQEQAQTERQETIFEIRARTQNIS. Descifrarea se va realizain mod similar folosind permutarea inversa σ−1. Daca dimensiunea transpozitiei N este mai mica decat lungimea parolei atunci se vor retine N caractere din parola.

Exercitiul 6. Studiati comutativitatea operatorilor de cifrare substitutie mono/polialfabetica si a transpozitiei.

Exercitiul 7. Implementati algoritmul de decriptare a unei transpozitii.

Exercitiul 8. Implementati algoritmul de decriptare a unei subtitutii simple.

Exercitiul 9. Implementati algoritmul de decriptare a unui cifru obtinut prin compunerea unei transpozitii si a unei substitutii simple.

Exercitiul 10. Implementati algoritmul de decriptare a unui cifru polialfabetic.