Digram substitution ciphers – cifruri cu substituție digrafică –

Cifrul Playfair

Informații generale

- Autor: Charles Wheatstone, în 1854;
- Promotor pe scară largă: Lyon Playfair;
- Lucrează prin substituirea, pe rând, a unor grupe de câte două litere conform unor reguli aplicate pe pătratul lui Polybius;
- Se bazează pe o parolă și pe o versiune modificată a pătratului lui Polybius (5 x 5) care folosește literele din parolă și restul literelor din alfabet;
- Alfabetul limbii engleze are 26 de litere (care trebuie găzduite în cele 25 de celule ale pătratului lui Polybius). Pentru a face posibil acest lucru se poate utiliza o anumită echivalență a unor perechi de litere;
- Familia de limbi germanice (inclusă engleza) folosește echivalența literelor I / J (Iohannis / Johannis)
- Familia de limbi romanice (latine) folosește echivalența literelor U / V (aqua / acva)

Cifrul Playfair criptează perechi de litere (cunoscute și sub termenul de *bigrame* sau *digrame*, în gr. *grama* = scrisoare), în loc de litere individuale, așa cum este cazul în cifrul cu substituție monoalfabetică (de ex. Caesar, ROT13, Vatsayana, etc.) sau polialfabetică (de ex. Vigenère).

Cifrul Playfair este semnificativ mai greu de spart, deoarece analiza de frecvență utilizată pentru cifrurile simple cu substituție nu funcționează în acest caz. Analiza de frecvență a bigramelor este posibilă, dar considerabil mai dificilă. Există 650 de bigrame posibile (perechile formate din aceeași literă dublată se exclud), adică semnificativ mai multe combinații decât cele 26 de monograme posibile (simboluri unice, de obicei litere în acest context), prin urmare efortul criptanalitic necesită un text cifrat considerabil mai mare pentru a fi util.

CONSTRUIREA PĂTRATULUI LUI POLYBIUS

Se alege o parolă pe baza căreia vom construi acest pătrat (5 x 5). De ex.

Parola: CORNEL

Pătratul lui Polybius (folosind echivalența I/J specifică limbii engleze) se completează folosind fiecare literă a alfabetului, o singură dată, începând însă cu literele din parolă. Apoi, vom completa restul literelor (rămase) din alfabet.

	1	2	3	4	5
1	C	O	R	N	E
2	L	A	B	D	F
3	G	H	I/J	K	M
4	P	Q	S	T	U
5	V	W	X	Y	Z

PREGĂTIREA TEXTULUI ÎN CLAR PENTRU OPERAȚIA DE CRIPTARE

Având pătratul construit putem trece la operația de pregătire pentru criptare a unui text în clar. Textul în clar (în eng. *plaintext*) se notează cu P. De ex.

P: ANA ARE MERE SI GUTUI

1. Se sparge textul în clar în grupe de câte două litere și vom obține **P: AN AA RE ME RE SI GU TU I**
2. Dacă textul în clar (spart în grupe de câte două litere) are o grupă incompletă (de ex. I), atunci se adaugă un caracter neutru la sfârșit (ținând cont de frecvența sa de apariție redusă, vom alege caracterul X și vom obține în exemplul precedent o digramă completă: IX). În acest moment, textul în clar este **P: AN AA RE ME RE SI GU TU IX**;
3. Dacă vreuna dintre grupe conține o literă dublată (de ex. AA), atunci cea de-a doua apariție a literei va fi înlocuită cu caracterul neutru (de ex. AX). **P: AN AX RE ME RE SI GU TU IX**

OPERAȚIA DE CRIPTARE

La sfârșitul operației de criptare se va obține textul cifrat (în eng. *ciphertext*, abreviat C). Fiecare digramă din textul în clar este substituită cu digrama corespondentă din textul cifrat conform următoarelor reguli.

P: **AN AX RE ME RE SI GU TU IX**
C: **DO BW NC UF NC XS MP UP SR**

1. Regula dreptunghiului/pătratului: perechea de vârfuri (plaintext) se substituie cu perechea de vârfuri rămasă (pe orizontală) pentru textul cifrat. De ex. perechea AN se substituie cu perechea DO (A se substituie cu D și N cu O).

	1	2	3	4	5
1	C	**O**	R	**N**	E
2	L	**A**	B	**D**	F
3	G	H	I/J	K	M
4	P	Q	S	T	U
5	V	W	X	Y	Z

2. Regula de linie: perechea de litere (din plaintext) identificată pe o aceeași linie se substituie cu literele deplasate la dreapta (pe aceeași linie – dacă este cazul prin rotire în spațiul aceleiași linii). De ex. perechea RE se substituie cu NC (R se substituie cu N și E cu C).

	1	2	3	4	5
1	**C**	O	**R**	**N**	**E**
2	L	A	B	D	F
3	G	H	I/J	K	M
4	P	Q	S	T	U
5	V	W	X	Y	Z

3. Regula de coloană: perechea de litere (din plaintext) identificată pe o aceeași coloană se substituie cu literele deplasate în jos (pe aceeași coloană – dacă este cazul prin rotire în spațiul aceleiași linii). De ex. perechea RE se substituie cu NC (R se substituie cu N și E cu C).

	1	2	3	4	5
1	C	O	R	N	**E**
2	L	A	B	D	**F**
3	G	H	I/J	K	**M**
4	P	Q	S	T	**U**
5	V	W	X	Y	Z

Textul cifrat va fi formatat în grupe de cinci litere pentru obfuscarea faptului că este vorba de cifrul Playfair.

P: **AN AX RE ME RE SI GU TU IX**
C: **DO BW NC UF NC XS MP UP SR**
C: **DOBWN CUFNC XSMPU PSR**

OPERAȚIA DE DECRIPTARE

Criptograful are la dispoziție parola (și își va construi pătratul lui Polybius respectând aceleași reguli) și textul cifrat. Algoritmul de decriptare aplică „invers" regulile folosite pentru criptare:

C: **DOBWN CUFNC XSMPU PSR**
C: **DO BW NC UF NC XS MP UP SR**
P: **AN AX RE ME RE SI/J GU TU I/JX**

1. Regula dreptunghiului/pătratului rămâne neschimbată. De ex. perechea DO se înlocuiește cu perechea AN;

	1	2	3	4	5
1	C	**O**	R	**N**	E
2	L	**A**	B	**D**	F
3	G	H	I/J	K	M
4	P	Q	S	T	U
5	V	W	X	Y	Z

2. Regula de linie se aplică în ordine „inversă" (adică prin substituirea literei de la dreapta cu cea din stânga). De ex. perechea NC se înlocuiește cu RE (litera N cu litera din stânga, adică R și litera C cu litera din stânga, adică E);

	1	2	3	4	5
1	**C**	O	**R**	**N**	**E**
2	L	A	B	D	F
3	G	H	I/J	K	M
4	P	Q	S	T	U

5	V	W	X	Y	Z

3. Regula de coloană se aplică de asemenea în ordine „inversă” (adică substituirea literei de jos cu cea de pe poziția imediat de mai sus). De ex. perechea UF se înlocuiește cu perechea ME (litera U cu litera de pe o poziție mai sus, adică M și litera F cu litera de mai sus, adică E).

	1	2	3	4	5
1	C	O	R	N	**E**
2	L	A	B	D	**F**
3	G	H	I/J	K	**M**
4	P	Q	S	T	**U**
5	V	W	X	Y	Z

Textul în clar obținut va fi analizat și reformatat (operațiile tipice implicând: analiza echivalențelor I/J, respectiv, sanitizarea textului ținând cont de semantică și utilizarea caracterului neutru).

C: **DOBWN CUFNC XSMPU PSR**
C: **DO BW NC UF NC XS MP UP SR**
P: **AN AX RE ME RE SI/J GU TU I/JX**
P: AN AA RE ME RE SI GU TU I => ANA ARE MERE SI GUTUI