

„Inelul $(\mathbb{Z}_n, +, \cdot)$ - aplicații interesante”

prof. VICTORIA POPA,
Colegiul Tehnic „Ion Mincu”, Timisoara

Algoritmul lui Gauss de aflare a datei Duminicii Paștelui

- Fie n anul în care se caută prima zi de Paște, zi notată cu x .
- Se determină următoarele resturi:
$$a \equiv n \pmod{19}$$
$$b \equiv n \pmod{4}$$
$$c \equiv n \pmod{7}$$
$$d \equiv (19a + 15) \pmod{30}$$
$$e \equiv (2b + 4c + 6d + 6) \pmod{7}$$
- Se calculează $x = d + e + 4$
- Dacă $x \leq 30$, atunci x se referă la o dată din aprilie, dacă $x > 30$, atunci x reprezintă o duminică din mai.

Exemplu: Vom calcula data primei zi de Paște în anul 2009, astfel:

$$n = 2009$$

$$a \equiv 2009 \pmod{19} \Rightarrow a = 14$$

$$b \equiv 2009 \pmod{4} \Rightarrow b = 1$$

$$c \equiv 2009 \pmod{7} \Rightarrow c = 0$$

$$d \equiv (19 \cdot 14 + 15) \pmod{30} \Rightarrow d = 11$$

$$e \equiv (2 \cdot 1 + 4 \cdot 0 + 6 \cdot 11 + 6) \pmod{7} \Rightarrow e = 4$$

$$x = d + e + 4 \Rightarrow x = 19$$

Deci, prima zi de Paște în anul 2009 va fi duminică, 19 aprilie.

Introducere în problematica securității informațiilor

Tehnicile de securizare a datelor au fost folosite încă de pe vremea vechilor egipteni. În cele două războaie mondiale ele au jucat un rol esențial. Până la mijlocul secolului XX principalii beneficiari ai unor asemenea tehnici au fost militarii, serviciile diplomatice și guvernele în general, ele fiind utilizate ca instrumente de protecție a strategiilor și a secretelor naționale.

Din 1960, odată cu proliferarea calculatoarelor și a comunicațiilor în domeniul privat, a apărut necesitatea protecției informațiilor în formă digitală. Începând cu 1997, datorită lucrărilor lui Fiestel la IBM, în SUA se adoptă un standard de criptare a informațiilor neclasificate – DES (Data Encryption Standard) care este, de altfel cel mai cunoscut sistem de securizare pentru comerțul electronic și în marile instituții financiare din lume.

În 1976 Diffie și Hellman introduc comerțul major de criptare în cheie publică, – metodă ingenioasă de schimb de chei- securizarea fiind bazată pe dificultatea inversării funcției logaritm discret, dar nu indică o tehnică de realizare practică. Acest lucru a fost făcut în 1978 de către Rivest, Shamir și Adleman, care indică prima schemă practică de criptare în cheie publică și de semnătură digitală – schemă folosită și acum și numită RSA. Schema RSA se folosește de o altă problemă matematică dificilă: factorizarea întregilor mari. Progrese aduc anii '80 când se pun în evidență cazuri când schema RSA este vulnerabilă. De asemenea, în 1985, El Gamal pune în evidență o clasă de scheme puternice în cheie publică folosind, de asemenea dificultatea inversării logaritmului discret. În anul 1991 apare primul standard internațional pentru semnătura digitală, provenit din schema RSA

(ISO/IEC 9796). În SUA guvernul adoptă în 1994 un standard de semnătură digitală bazat pe schemele de cheie publică El Gamal.

Între timp au apărut noi scheme de securitate a datelor, toate având ca suport probleme de matematică computațională.

De-a lungul timpului s-au elaborat protocoale și mecanisme cu scopul securizării informației, atunci când informația este transportată prin documente fizice. Adesea obiectivele securității informației nu pot fi soluționate doar prin algoritmi matematici și protocoale; sunt necesare și tehnici procedurale precum și respectarea regulilor (oficiale sau neoficiale) de acțiune în vederea atingerii scopului vizat. De exemplu confidențialitatea unei scrisori este asigurată de plicul livrat de un serviciu poștal acceptat. Securitatea fizică a plicului este, practic, limitată și astfel apar legi emise cu scopul de a preveni deschiderea acestuia de către persoane neautorizate.

Modul de înregistrare a informației s-a schimbat esențial. Inițial, datele erau stocate pe hârtie și transmise prin plicuri. Acum informația se stochează pe suport magnetic sau optic și se transmite prin diferite sisteme de telecomunicații, tot mai des fără fir. S-a schimbat, de asemenea, radical abilitatea de copiere ori alterare a informației. Se pot face mii de copii a unei pri de informație stocat electronic și acestea nu pot fi autentificate față de original. Prin urmare, într-o societate în care informația este stocată și transmisă electronic, este necesar asigurarea securității datelor independent de mediul fizic de înregistrare ori de transport.

Un instrument fundamental utilizat în securizarea datelor este semnătura. Există blocuri informaționale care asigură și alte servicii ca nonrepudierea, autentificarea originii datelor, identificare ori atestarea. Semnătura, pe lângă alte cerințe, trebuie să fie unic atașată unei entități și servește la indentificare, autorizare și validare.

De asemenea, sunt necesare analoagele protocoalelor scrise pe hârtie în variantă electronică; astfel de protocoale sunt fără îndoială mai bune decât cele clasice.

Realizarea securității informației în această perioadă impune un instrumentar vast de tehnici legale ingenioase; acestea sunt oferite de *criptografie* – înțelesă aici ca studiul procedurilor matematice legate de aspecte ale securității informațiilor cum ar fi: *integritatea datelor*, *confidențialitatea*, *autentificarea entităților*, *autentificarea originii datelor*.

Criptarea și decriptarea mesajelor cu cifrul lui Cezar

Una dintre cele mai cunoscute tehnici de criptare este cifrul lui Cezar, care folosește o permutare circulară pe literele alfabetului latin cu o cheie $k \in [0,25]$ în mulțimea Z_{26} :

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

Pentru criptarea mesajului este folosită o funcție bijectivă $e_k(\alpha) = (\alpha + k)(\text{mod } 26)$, unde k reprezintă cheia de criptare, $k \in [0,25]$, iar α reprezintă numărul corespunzător literei din mesajul care va fi criptat.

Pentru exemplificare, vom cripta mesajul „SIMPOZION” cu cheia $k=11$. Vom calcula:

$$e_{11}(S) = (11+18)(\text{mod } 26) = 3 \Rightarrow D$$

$$e_{11}(I) = (11+8)(\text{mod } 26) = 19 \Rightarrow T$$

$$e_{11}(M) = (11+12)(\text{mod } 26) = 23 \Rightarrow X$$

$$e_{11}(P) = (11+15)(\text{mod } 26) = 0 \Rightarrow A$$

$$e_{11}(O) = (11+14)(\text{mod } 26) = 25 \Rightarrow Z$$

$$e_{11}(Z) = (11+25)(\text{mod } 26) = 10 \Rightarrow K$$

$$e_{11}(N) = (11+13)(\text{mod } 26) = 24 \Rightarrow Y$$

Astfel, mesajul criptat devine : „DTXAZKTZY”

Pentru decriptarea mesajului, se folosește funcția $d_k(\beta) = (\beta - k)(\text{mod } 26)$, unde k reprezintă cheia de decriptare, iar β reprezintă numărul corespunzător literei din mesajul de decriptat.

Pentru exemplificare, vom decripta mesajul „DTXAZKTZY” cu cheia $k=11$.

$$d_{11}(D) = (3-11)(\text{mod } 26) = (3+15)(\text{mod } 26) = 18 \Rightarrow S$$

$$d_{11}(T) = (19-11)(\text{mod } 26) = (19+15)(\text{mod } 26) = 8 \Rightarrow I$$

$$d_{11}(X) = (23-11)(\text{mod } 26) = (23+15)(\text{mod } 26) = 12 \Rightarrow M$$

$$d_{11}(A) = (0-11)(\text{mod } 26) = (0+15)(\text{mod } 26) = 15 \Rightarrow P$$

$$d_{11}(Z) = (25-11)(\text{mod } 26) = (25+15)(\text{mod } 26) = 14 \Rightarrow O$$

$$d_{11}(K) = (10-11)(\text{mod } 26) = (10+15)(\text{mod } 26) = 25 \Rightarrow Z$$

$$d_{11}(Y) = (24-11)(\text{mod } 26) = (24+15)(\text{mod } 26) = 13 \Rightarrow N$$

Astfel, mesajul decriptat devine : „SIMPOZION”.

Criptarea și decriptarea mesajelor cu sistemul Cardano

Sistemul Cardano este un sistem de criptare autosincronizabil cu cheie fluidă. Un sistem de criptare se numește autosincronizabil, dacă un caracter al cheii fluide se construiește nu numai cu ajutorul cheii k , ci și cu ajutorul unui număr fixat de caractere criptate în prealabil. Sistemul Cardano folosește pentru criptare o cheie fluidă $z_1 = k, z_{i+1} = y_i, i \geq 1$, unde y reprezintă mesajul criptat (literele obținute în urma criptării), iar x reprezintă mesajul clar (ce urmează a fi criptat).

Pentru exemplificare, vom cripta cu cheia fluidă $z_1 = 15 = k$ mesajul „MONOID”. Utilizăm literele alfabetului latin, iar operațiile se efectuează în Z_{26} . De fiecare dată, se adună mesajul criptat obținut anterior, ca mai jos:

	M	O	N	O	I	D
x	12	14	13	14	8	3
z=15	15	1	15	2	16	24
y	1	15	2	16	24	1
	B	P	C	Q	Y	B

Pentru decriptare, se folosește $x_1 = y_1 - k, x_i = y_i - y_{i-1}, i \geq 1$. Pentru exemplificare, vom decripta mesajul „BPCQYB”, utilizând scăderea ca adunarea cu opusul în Z_{26} . Prin calcul, obținem următoarele date, pe care le atașăm schemei de decriptare de mai jos.

$$x_1 = (1 - 15)(\text{mod } 26) = 1 + 11 = 12$$

$$x_2 = y_2 - y_1 = (15 - 1)(\text{mod } 26) = 15 + 25 = 14$$

$$x_3 = y_3 - y_2 = (2 - 15)(\text{mod } 26) = 2 + 11 = 13$$

$$x_4 = y_4 - y_3 = (16 - 2)(\text{mod } 26) = 16 + 24 = 14$$

$$x_5 = y_5 - y_4 = (24 - 16)(\text{mod } 26) = 24 + 10 = 8$$

$$x_6 = y_6 - y_5 = (1 - 24)(\text{mod } 26) = 1 + 2 = 3$$

	B	P	C	Q	Y	B
y	1	15	2	16	24	1
k=15	15	1	15	2	16	24
x	12	14	13	14	8	3
	M	O	N	O	I	D

Am obținut mesajul decriptat „MONOID”.

Bibliografie

D. Săvulescu ș.a.- Manual matematică, cls. a XII-a, Ed. Art

L. Niculescu ș.a.- Manual matematică, cls. a XII-a, Ed. Cardinal

D. Dăianu- „Bazele matematice ale securității în tehnologia informației”, Ed. Politehnica, 2006

D. Dăianu- „Bazele matematice ale securității în tehnologia informației”-suport de curs master
„Algoritmi avansați de matematică cu aplicații în inginerie și economie”, Universitatea Politehnica
Timișoara