# Exerciții competiție studențească

Prof.dr. Ferucio Laurenţiu Ţiplea
Department of Computer Science
"Alexandru Ioan Cuza" University of Iaşi
e-mail: ferucio.tiplea@uaic.ro

## Problema 1: Lungimea cheii de criptare

Presupunem că criptăm texte scrise folosind alfabetul limbii engleze fără a face distincție între litere mici și mari. Ca urmare, neglijăm și diacriticele (dacă, de exemplu, criptăm texte în limba română folosind acest alfabet). Alfabetul acesta are 26 de caractere, numerotate de la 0 la 25.

Tehnica de criptare este următoarea:

1. generăm o cheie $K$ ca o secvență de $\ell > 1$ numere între 0 și 25;
2. caracterele (din text) de pe pozițiile 1, $\ell + 1$, $2\ell + 1$ etc. se permută circular cu $K(1)$ poziţii. De exemplu, caracterul "a" permutat circular cu 3 poziţii se înlocuieşte cu "d", iar "y" cu "b";
3. caracterele (din text) de pe pozițiile 2, $\ell + 2$, $2\ell + 2$ etc. se permută circular cu $K(2)$ poziţii;
4. procesul descris mai sus se continuă până se criptează tot mesajul (presupunem că cheia de criptare este mai scurtă decât mesajul, cu toate că această cerinţă nu este absolut necesară).

Textul criptat de mai jos a fost obtinut prin procedura descrisă mai sus cu o cheie ce nu depăşeşte 10 caractere dar are măcar 5 caractere. Care este lungimea ei?

ORLNHTWJDPBZGURWXSZRKIHTCZZTVOWJCLXRKULDMORGPDIFKRR
TEMNVYGGTQIRWXGCBCDYQQIPTVHPVQHMVGICLTGPFNXMMHFPJLV
QNCKXFYVUXEZUKSSRAQICSNFKEEIAWUJCBXGVVPIHDCJQIASGOYB

**Soluţeie:** "QI" apare la poziţiile 61, 73, 121 şi 147. Distanţele între ele sunt 12, 48 şi 26. Divizorii comuni sunt 1 şi 2, ceea ce nu asigură lungimea corespunzătoare a cheii. Ne uităm atunci la divizorii pentru 12 şi 48. Aceştia sunt 1, 2, 3, 4, 6 şi 12. Soluţia este atunci 6.

**Problema 2: Transfer bancar**

Presupunem că sistemul de criptare pe care il folosim în continuare este de următorul tip:

1. dat un mesaj (text, formular etc.) ca o secvenţă de octeţi, se generează random octet după octet şi se face XOR cu octeţii textului în ordinea în care aceştia apar în text;

2. octeţii generaţi, în ordinea generării, reprezintă cheia de criptare. Ea va fi salvată de criptor şi transmisă la decriptor printr-o metodă care nu ne interesează momentan.

Prespunem că această tehnică de criptare se utilizează la criptarea unor formulare ce conţin în ultimele două câmpuri numele unei persoane şi apoi contul bancar al acesteia. Formularul specifică un transfer bancar către persoana şi contul specificate în ultimele două câmpuri.

Cum poate un adversar ce are acces la canalul de comunicaţie, ştiind că unei cunoştinţe a lui, pentru care el cunoaşte numele şi contul bancar, urmează să i se facă un transfer bancar printr-un astfel de formular criptat, să modifice formularul criptat fără a cunoaşte cheia de decriptare astfel încât suma de bani să fie transferată în contul lui.

**Soluţie:** Dacă adversarul a obţinut un formular criptat al unei persoane pentru care ştie numele şi contul bancar (acestea nu sunt informaţii secrete), atunci construieşte un mesaj de aceeaşi lungime cu cea a formularului dar care are numai 0 în prima parte, iar la final are:

$$nume\_persoana\_cont\_persoana \; XOR \; nume\_adversar\_cont\_adversar$$

Acest formulat, făcut XOR cu formularul criptat obţinut de adversar conduce la cerinţa problemei.