Teme laborator

1. Scrieti un program care primeste ca input un text m de maxim 50 de caractere si un numar natural n(n <= lungimea textului m). Programul trebuie sa determine 2 lucruri:
   1. Sa verifice daca textul m poate fi un text criptat cu playfair. Programul va afisa un raspuns “DA” sau “NU” si motivul pentru care nu poate fi un text criptat cu playfair.
   2. Sa realizeze un atac de tip forta bruta pentru a determina cheia utilizata la criptare stiind ca n este dimensiunea cheii. Programul va afisa mesajele decriptate cu cheile determinate.
2. Se da un numar N de maxim 200 de cifre, produsul a doua numere prime p si q cu:

|p – q | < 2

Gasiti cei doi factori primi p si q.

1. Se trimite un mesaj intre 2 banci din Romania care reprezinta un transfer de suma si are formatul de mai jos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Banca A | Cont A | Banca B | Cont B | Suma | Valuta |

Fiecare bloc este criptat cu AES mod ECB.

Scrieti un program care realizeaza cel putin urmatoarele:

* 1. Citeste din fisier sau baza de date conturile in format iban intre care se face transferul, suma si valuta. Banca se poate determina din iban (ex: pentru ibanul RO 06 INGB 0001 0001 8824 8913 banca este ING deoarece codul bic INGB corespunde ING).
  2. Cripteaza mesajul cu AES in mod ECB si scrie mesajul intr-un fisier text
  3. Simuleaza un atac al lui Oscar, acesta dorind sa trimita banii in contul lui de la Banca B. Fisierul text cu mesajul criptat este modificat astfel incat banii sa ajunga in alt cont nestiind cheia de criptare.

Puteti alege AES pe oricati biti doriti. Puteti folosi pentru AES biblioteci deja implementate in tehnologia aleasa.