Criptare si decriptare

1. **Problema**

Alice si Bob vor sa comunice sigur, astfel ca utilizeaza structuri algebrice pentru crearea unui mod de a cripta mesajele. Modul lor de lucru se bazeaza pe urmatorul argument matematic: daca 𝑝 este un numar prim, atunci grupul multiplicativ al unitatilor (ℤ𝑝∗,⋅) este ciclic si este izomorf cu grupul aditiv (ℤ𝑝−1,+). Izomorfismul este dat imediat daca se cunoaste un generator al grupului multiplicativ: fie 𝑔 ∈ ℤ𝑝∗ un generator (i.e. ℤ𝑝∗ ≔< 𝑔 >; 𝑔 este generator daca si numai daca puterile lui mod 𝑝 genereaza toate elementele din grupul multiplicativ al unitatilor), atunci fiecarui element din ℤ𝑝−1 ii corespunde un element din ℤ𝑝∗ dupa regula: ∀𝑥 ∈ ℤ𝑝−1 ∃!𝑦 = 𝑔𝑥−1 ∈ ℤ𝑝∗

1. **Cerinte**

1. Se citeste un numar 𝑝 de la tastatura. Sa se determine generatorul (cel mai mic) 𝑔 astfel incat ℤ𝑝∗ ≔< 𝑔 > (adica sa se determine generatorul cu proprietatea de mai sus: ridicat succesiv la putere, modulo numarul citit 𝑝, sa genereze toate elementele de la 1 la 𝑝 − 1). Atentie! Nu se garanteaza faptul ca 𝑝 este dat mereu corect (adica numar prim), trebuie testata initial aceasta conditie. Daca 𝑝 NU este prim, se va afisa un mesaj corespunzator pe ecran, altfel se va afisa un mesaj de forma (Generatorul g este: ...).

2. Dat un mesaj clar, sa se cripteze.

3. Dat un mesaj criptat, sa se decripteze.

1. **Descriere solutie**

* Registrii utilizati: $t0 – p, $t1 – g (generator), $t2 - $t5 (diverse valori pe parcursul programului)
* Pas 1: citirea datelor (p, s1, s2)
* Pas 2: verificare daca p e nr prim
* prima data verific daca p este 1 (caz in care nu este prim) sau 2
* apoi verific daca p este multimplu de 2, in cazul in care p != 2 (daca da => p nu e prim)
* dupa aceea iau toate valorile impare de la 3 la sqrt(p) si verific daca il divid pe p (daca p are divizori proprii => nu e prim)
* daca p nu este prim se afiseaza mesajul “p nu e prim”
* daca p este prim se trece la urmatorul pas
* Pas 3: determinarea generatorului
* se observa ca un numar din intevalul [2, p-1] este generator in grupul multiplicativ al unitatilor lui p daca puterea la care acesta da valoara 1 este p-1 (pe aceasta observatie se bazeaza metoda mea de determinare a celui mai mic generator)
* in memorie pastrez un vector (put) in care retin valorile puterilor generatorului, ce are pe pozitia 0 valoarea 1
* pentru fiecare i din intervalul [2, p-1] calculez valoarile puterilor lui i in grup (dupa formula: ij = (ij-1 \* i) % p) pe care le adaug in vectorul de puteri, pana cand obtin valoarea 1 (aceasta nemaifiind adaugata in vector)
* verific daca puterea lui i la care se obtine valoarea 1 este p-1: in caz afirmativ i este cel mai mic generator al grupui si se trece la pasul urmator, iar in caz negativ se creste valoarea lui i si se reia procesul descris anterior
* odata gasit generatul, se afiseaza mesajul “Generatorul g este: “ si valoarea acestuia
* Pas 4: criptarea
* am retinut in memorie un sir (alf) alcatuit din literele mari ale alfabetului englez (acesta o sa fie folosit pentru o determinare mai usoara a caracterului criptat)
* pentru fiecare caracter din sirul s1 calculez valoarea diferentei dintre codul sau ASCII si codul ASCII al caracterului ‘A’, aceasta reprezentand pozitia in vectorul de puteri
* caut in vectorul de puteri valoarea de pe pozitia caluculata anterior, aceasta valoare va reprezenta pozitia in sirul alf a carcaterului corespunzator criptarii caracterului din sir
* afisez caracterul de pe pozitia respectiva din sirul alf
* Pas 5: decriptarea
* o sa folosesc acelasi sir alf pentru a determina fiecare caracter decriptat
* pentru fiecare caracter al sirului s2 calculez diferenta dintre codul sau ASCII si codul ASCII al caracterului ‘A’, aceasta diferenta va reprezenta o valoare din vectorul de puteri ale lui g
* caut pozitia pe care se afla valoarea calculata anterior in vectorul de puteri, aceasta reprezentand pozitia din sirul alf a caracterului corespunzator decriptarii caracterului din sir
* afisez caracterul de pe pozitia respectiva din sirul alf
* Pas 6: iesire program

1. **Exemple**

* p = 7 s1 = ACAD s2 = BCBG

=> Generatorul g este: 3

Mesajul criptat este: BCBG

Mesajul decriptat este: ACAD

* p = 8 s1 = ADB s2 = HGF

=> p nu este prim

* p = 13 s1 = DAFEK s3 = GJLEI

=> Generatorul g este: 2

Mesajul criptat este: IBGDK

Mesajul decriptat este: FIHCD

* p = 23 s1 = ARES s3 = RAGE

=> Generatorul g este: 5

Mesajul criptat este: BPEG

Mesajul decriptat este: HXSE

* p = 0 s1 = ARES s3 = RAGE

=> p este 0 sau negativ