Studierea sistemului criptografic simetric ElGamal

DANILOV A. AND CHIRIAC L.

În prezent tehnicile de criptare sunt omniprezente și sunt utilizate, în realizarea diverselor operațiuni cotidiene: securizarea plăților on line, asigurarea confidențialității discuțiilor prin intermediul telefoanelor mobile, securizarea operațiunilor efectuate prin intermediul cardurilor bancare, securizarea implementării votului electronic. Cei mai siguri algoritmi criptografici au la bază o serie de concepte matematice. Astfel, pentru a înțelege funcționarea acestor algoritmi este necesară înțelegerea conceptelor matematice respective. Așa cum în viitorul apropiat centrul de greutate a cercetărilor în domeniul informaticii se va transfera pe segmentul algoritmilor criptografici, este necesar de menționat faptul că pregătirea specialiștilor informaticieni de clasă înaltă presupune, în opinia noastră, pregătirea fundamamentală în domeniul algebrei abstracte și teoriei numerelor. Aplicații practice, în acest sens, adică elaborarea și implemntarea programelor bazate pe concepte matematice moderne va trezi un interes sporit din partea studenilor și masteranzilor în raport cu acest domeniu de mare perspectivă. În această lucrare, autorii demonstrează și ilustrează din punct de vedere metodologic, necesitatea cunoașterii conceptelor matematice pentru înțelegerea funcționării și utilizării unui apreciat sistem criptografic, cunoscut în literatura de specialitate ca sistemul criptografic El Gamal. Sistemul criptografic ElGamal este cu cheie publică și se bazează pe ”dificultatea” calculării valorilor logaritmilor discreți pe așa structuri algebrice precum corpuri finite. Sistemul criptografic ElGamal include: algoritmul de criptare ElGamal și algoritmul semnăturii dijitale.

(DANILOV A., CHIRIAC L.) UNIVERSITATEA DE STAT DIN TIRASPOL