Ministerul Educaţiei, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

**RAPORT**

Lucrarea de laborator nr. 6 La Criptografie V:7

A efectuat: Șeremet Alexandru

A verificat: Andronatiev Victor

Chișinău - 2022

**Sarcina nr.1(RSA)**



-Aflam varianta



Varianta 7 : SHA-1

-Alegem p si q 2 nr prime



-Aflam n, produsul dintre p si q



-Verificam daca lungimea lui este mai mare sau egala cu 3072



-Aflam fi=(p-1)(q-1)



-Cu ajutorul lui fi il aflam pe e, e se obtine ca fiind cel mai mic numar dintre fi modulo si care nu da in rezultat 0



-Aflam hashul mesajului in SHA-1 dupa care il transformam in decimal

-Aflam d dupa formul e-1mod(fi)



Mesajul



Hashul mesajului



Hashul transformat in decimal



-Cream semnatura digitala cu ajutorul formulei hasm10dmod(n)



-Decriptam mesajul cu ajutorul semnaturii dupa formula semod(n)



-Verificam daca mesajul decriptat este identic cu hashul in decimal



**Sarcina nr.2(ELGAMAL)**

-Sarcina



-Alegem hashul corespunzator variantei

MD6-512

-Criptam mesajul cu hashul dat



-Transformam hashul in decimal



-Introducem p si g din datele laboratorului



-Alegem un numar z aleatoriu dupa care aflam Beta dupa formula gzmod(p)



-Alegem un numar k comun care e cel mai mic divizor al lui p-1 si in urma operatiei (p-1)mod(k) nu vom obtine 0



-Aflam elementul r prin formula gkmod(p)



-Aflam semnatura digitala dupa formula

**[(hashm10E-z\*r)\*k-1mod(p-1)]mod(p-1)**



-Aflam v1 dupa formula **[Betarmod(p)\*rsmod(p)]mod(p)**



-Aflam v2 dupa formula ghashm10Emod(p)



-Verificam daca v1 este egal cu v2mod(p)

