Lucrare de laborator nr. 5

CRIPTOGRAFIA CU CHEI PUBLICE

Sarcina 1. Studiați materiale didactice recomandate la temă plasate pe ELSE.

***Sarcina* 2.1. Utilizând platforma *wolframalpha.com* sau aplicația *Wolfram Mathematica*, generați cheile și realizați criptarea și decriptarea mesajului**

m* = *Nume Prenume

aplicând algoritmul RSA.
Valoarea lui *n* trebuie să fie de cel puțin 2048 biți.

***Sarcina* 2.2. Utilizând platforma *wolframalpha.com* sau aplicația *Wolfram Mathematica*, generați cheile și realizați criptarea și decriptarea mesajului**

m* = *Nume Prenume

aplicând algoritmul ElGamal (*p* și *generatorul* sunt dați mai jos).

***Sarcina* 3. Utilizând platforma *wolframalpha.com* sau aplicația *Wolfram Mathematica*, realizați schimbul de chei Diffie-Helman între Alisa și Bob, care utilizează algoritmul AES cu cheia de 256 de biți.**
Numerele secrete *a* și *b* trebuie să fie alese în mod aleatoriu în conformitate cu cerințele algoritmului (*p* și *generatorul* sunt dați mai jos).

Notă:

Pentru sarcinile 2.1 și 2.2 utilizați reprezentarea numerică zecimală a mesajului, ajungând la aceasta prin reprezentarea hexazecimală a caracterelor, în conformitate cu codificarea ASCII. Pentru comoditate în conversie puteți să vă folosiți de pagina https://www.rapidtables.com/convert/number/hex-to-decimal.html.

Pentru sarcinile 2.2 și 3 considerași

p=32317006071311007300153513477825163362488057133489075174588434139269806834136210002792056362640164685458556357935330816928829023080573472625273554742461245741026202527916572972862706300325263428213145766931414223654220941111348629991657478268034230553086349050635557712219187890332729569696129743856241741236237225197346402691855797767976823014625397933058015226858730761197532436467475855460715043896844940366130497697812854295958659597567051283852132784468522925504568272879113720098931873959143374175837826000278034973198552060607533234122603254684088120031105907484281003994966956119696956248629032338072839127039,

care are 2048 biți și generatorul *g*=2.

Raportul trebuie însoțit de comentarii detaliate ale tuturor pașilor algoritmilor.

Funcții utile în Wolfram:

- ***Prime*[*n*] –** *returnează al n-lea număr prim din lista numerelor prime (n este mărginit);*
- ***RandomPrime*[{i_{min}, i_{max}}] –** *returnează un număr prim pseudoaleator cuprins între* i_{min} *și* i_{max} *;*
- ***RandomInteger*[i_{max}] –** *returnează un număr întreg pseudoaleator cuprins între 0 și* i_{max} *;*
- ***Mod[a, n] –** returnează restul împărțirii lui a la n;*
- ***PoerMod[a, b, n] –** returnează restul împărțirii lui* a^b *la n;*
- ***FactorInteger [n] –** returnează lista de factori primi ai lui n, împreună cu exponenții lor;*
- ***IntegerDigits[n, b] –** returnează lista de cifre în baza b a numărului întreg n;*
- ***Length[lst] –** returnează lungimea listei lst;*