Ministerul Educaţiei, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

**RAPORT**

Lucrarea de laborator nr. 5 La Criptografie

A efectuat: Șeremet Alexandru

A verificat: V Andronatiev

Chișinău - 2022

Lucrare de laborator nr. 5.

Tema: CRIPTOGRAFIA CU CHEI PUBLICE

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

***Sarcin*a 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.**

***Sarcin*a 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).**

***Sarcin*a 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**](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.

Mersul lucrări:

RSA

Aflam p și q



p=RandomPrime[{2^1030, 2^1050}]

5964422578360289643577482894101648319028774001007546800762626861559139872767541967428867355533904214060600975434653312258869200619521324528573043721757436716826908198121054401747388649043858745599323534425995417687072694910021916758009449190095080745858541031620505762923834348954848135858169730346205347360105589957

q=RandomPrime[{2^1030, 2^1050}]

2252147139642425488965409823029149840268695704031953743357367400391621932744387764717990952408351994557106285819519818921657613874889142423131615244050303074122694539031475080178431618613433651816333216209479946546458055972915784537123542966274164166808247436340580419950650246228785136875702394243608203073135666983

Verificarea lunginea lui p si q

Length[IntegerDigits[p,2]]

1049

Length[IntegerDigits[q,2]]

1048

Aflarea n dupa formula n=p\*q



n=p\*q

13432757249472826723293797284714950571428791844883908989801528175124138576208082505464263870282698028841758051845653561106550465357702648337643186140144148397439865262398328045547814013865983518984774577033313063588865325856223988946646544404614377298998677615019129267182996487686704863003582355024592691911043107092374254339993240438710637208380764245582352744237304327264938436127157105352800593093337147074085664491627624561806986744898506582546827559468657615741645157885547069804454643863689569422941264334859549730859280251053663353465399052615257819179367994039327473768856316739627539613619228004357299942137877811901289731

Verificarea lungimea valoarea lui n trebuie să fie de cel puțin 2048 biți.

Length[IntegerDigits[n,2]]

2097

Calcularea lui Fi



f=(p-1)\*(q-1)

13432757249472826723293797284714950571428791844883908989801528175124138576208082505464263870282698028841758051845653561106550465357702648337643186140144148397439865262398328045547814013865983518984774577033313063588865325856223988946646544404614377298998677615019129267182996487686704863003582355024592691911043107084157684621990525306167744491249966086284883039197803783144944174176395299840870860946478839131829455873920363307633855564371692088136360607763998649933905366935944332651925161937869301765648866919202799095383916017522912470527697757482265662810123081372539005807770133865142944429985955270485175352324327378660032792

e=FactorInteger[f]

$Aborted

Aflarea numarului e. Daca funcțiea FactorInteger[f] nu funcționează folosim metoda de mai jos



Mod[f ,5]

2

e=5

5

Mesajul si convertarea lui

m="Seremet Alexandru";

m16="43686972697461205374616E69736C6176"

43686972697461205374616

m10=22937705806984324019616246073949843906934

22937705806984324019616246073949843906934

Mesajul Criptat

c=PowerMod[m10,e, n]

6349651525128921555677530474896850317413728619458942728783746844066889508263262462743511409395786351422586054223468108551452968152372067280545089911537465437766708774379742590835976137281521072375427424

Calcularea cheiei secrete.



d=PowerMod[e,-1,f]

5373102899789130689317518913885980228571516737953563595920611270049655430483233002185705548113079211536703220738261424442620186143081059335057274456057659358975946104959331218219125605546393407593909830813325225435546130342489595578658617761845750919599471046007651706873198595074681945201432942009837076764417242833663073848796210122467097796499986434513953215679121513257977669670558119936348344378591535652731782349568145323053542225748676835254544243105599459973562146774377733060770064775147720706259546767681119638153566407009164988211079102992906265124049232549015602323108053546057177771994382108194070140929730951464013117

Decriptarea mesjului.



dec=PowerMod[c,d,n]

22937705806984324019616246073949843906934

Verificarea daca sunt identice.

dec==m10

True

Diffie-Hellman

Numar p și g sunt date din condiți.

p1= 3231700607131100730015351347782516336248805713348907517458843413926980683413621000279205636264016468545855635793533081692882902308057347262527355474246124574102620257916572972862706300325263428213145766931414223654220941111348629991657478268034230553086349050635557712219187890332729569696129743856241741236237225197346402691855797767976823014625397933058015226858730761197532436467475855460715043896844940366130497697812854295958659597567051283852132784468522925504568272879113720098931873959143374175837826000278034973198552060607533234122603254684088120031105907484281003994966956119696956248629032338072839127039

3231700607131100730015351347782516336248805713348907517458843413926980683413621000279205636264016468545855635793533081692882902308057347262527355474246124574102620257916572972862706300325263428213145766931414223654220941111348629991657478268034230553086349050635557712219187890332729569696129743856241741236237225197346402691855797767976823014625397933058015226858730761197532436467475855460715043896844940366130497697812854295958659597567051283852132784468522925504568272879113720098931873959143374175837826000278034973198552060607533234122603254684088120031105907484281003994966956119696956248629032338072839127039

g=2

2

Calculam cheia privata lui Bob



BobKeyPrivate=RandomInteger[p1]

3175601716335130482926949396725198142120263057484746069600456575583225478776694177360604087564449323141984883278260738054248196826493945809904980190778337006819841633643640974666031013291040490583969285376431927569152028254165155616328765804068982954790316110499452523107923205093421280095972868825445906157610482548539651876528520734090843766728267108527817789689545684798932323020602403114197768065810936718660664494842516871834564335168125794585708801242312962703682981217401551088261028852998497936694298753413401344620910303041780498693913830862897780896298013045791797902202361877497261409587393971930377453268

Calculam cheia privata lui Alice



AliceKeyPrivate=RandomInteger[p1]

651740657701959250288934723217133439966832936819738486906203663286774849066694156401787406508038272078153201378705777265669058192859658074986226008255531194242530738580170486332106194710978270430337318981067224043634762631842648766800624246705668997184525716162646820155231231836936247129810759366055790895591126521587756398293923094771815371545668162088987071547172363575866203202421299931879396184253543772485707293701992678564249195361882961989367847808581191314332011833122857018721521682460322026611312689244278132137056032022716384591443603189508917818182320555613474626643200745888100672936912007754504480513

Calculam cheia privata lui Bob



BobKeyPublic=PowerMod[g,BobKeyPrivate,p1]

38707251398289360428552393428378738712279530690238400574372307385435842212708853527351312319415298216447733352836311758450265825280912780960079457273575158223330117611100737078293103997360671837431128459660370892527407769746278927663354756424181300396197030213309411560555376062944923309653307271206827127630971987599274760563359842103434363720959176910318486821237678827832289205656964807024588206181288081296230024625975468828231049057963534784457953100659801501433541029910834400722749555315548361141960678666347765606896852575419859579038207524748678375279945586788579812073284463195905886596801136489888541017



AliceKeyPublic=PowerMod[g,AliceKeyPrivate,p1]

2377820197940222483961609410441153200642587322027807844954858568241159830750515477586455314827149132343415431590398017463167149281650720729950859687794483996959409124803352291782901549594699931257280246022136787318482589555831200555690859468325856044496171423883762517294522077923468122656832309960565670729179261195356034175774529188459737465438491975207014820185803051508132258675950534131099896720879898313054179108809870904355341375549121626324437021469856430379779866340120620312660369154335499011844784907952257873296281233370442896721010755866457405830478872538645712832841883984631526789060193980103806527352

Schimb de chei

K1=PowerMod[BobKeyPublic,AliceKeyPrivate,p1]

2593671287325355599639898495090028409368155808500711980190168602969102578702117175040672419291884366828223397495181654470925972631038725560339451582901540707315985825564396877649773867730875096842094251744122604074014828783951342647110885416956038842270711598736385266734771228567600727715595834468284326486482309084169752581013531559283304272782579569246557242449967048559797364808143605676378292071663688603813564908845518143614997167708548173438260686274247879081938942411404839159895035919806033856981541481122272821235630285921803661833465119876336811176074558571865287572903421127934088605022024568809180006092

K2=PowerMod[AliceKeyPublic,BobKeyPrivate,p1]

2593671287325355599639898495090028409368155808500711980190168602969102578702117175040672419291884366828223397495181654470925972631038725560339451582901540707315985825564396877649773867730875096842094251744122604074014828783951342647110885416956038842270711598736385266734771228567600727715595834468284326486482309084169752581013531559283304272782579569246557242449967048559797364808143605676378292071663688603813564908845518143614997167708548173438260686274247879081938942411404839159895035919806033856981541481122272821235630285921803661833465119876336811176074558571865287572903421127934088605022024568809180006092

Verificarea lungimi lui k1

Length[IntegerDigits[K1,2]]

2045

Reprezentarea lui k1 în forma de biți

Kbin=IntegerDigits[K1,2]

{1,0,1,0,0,1,0,0,0,1,0,1,1,1,0,1,1,1,0,1,1,1,1,0,0,1,0,1,0,1,1,0,0,0,1,1,1,0,1,1,1,0,0,1,1,0,0,1,0,0,0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,1,1,1,0,1,0,0,1,0,1,1,1,1,0,0,1,0,0,1,0,0,1,0,0,1,1,1,0,1,1,0,1,0,1,0,0,0,1,0,1,0,0,0,1,1,1,0,1,0,0,0,0,1,1,0,1,0,0,0,1,0,1,0,0,0,1,0,0,1,0,1,0,0,1,1,0,0,0,0,0,1,1,1,0,1,0,0,0,0,1,1,1,0,0,1,1,1,1,0,0,1,0,1,0,1,0,0,1,1,0,1,0,0,1,0,0,1,0,0,1,0,0,1,1,0,1,1,0,1,1,1,1,0,1,1,0,1,0,0,0,1,0,0,1,0,0,0,1,1,1,0,0,1,0,0,0,0,0,0,0,0,1,1,0,1,1,0,1,1,0,1,0,1,0,0,1,1,1,1,0,1,1,1,0,0,1,0,0,1,0,1,0,0,0,0,1,0,0,1,0,0,1,1,0,1,0,1,1,0,1,0,0,1,0,1,1,0,0,1,1,0,1,1,1,1,0,1,0,1,1,1,0,1,1,1,1,0,0,1,1,1,0,1,0,1,0,0,0,0,1,0,1,0,1,0,1,1,1,0,0,1,0,1,0,1,0,1,1,0,1,0,0,1,1,0,1,1,0,1,0,1,1,1,0,1,0,1,0,1,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,0,1,0,1,0,1,0,0,0,1,1,0,0,1,1,1,0,1,0,0,0,1,1,1,0,1,0,0,0,1,1,1,1,1,1,1,0,0,1,1,0,1,1,0,1,0,0,0,1,1,1,1,0,1,1,0,0,0,1,1,0,1,0,0,1,0,0,1,1,1,1,0,1,0,1,1,1,1,1,0,1,1,0,1,0,1,0,0,1,1,0,0,0,0,0,1,0,0,0,1,1,1,1,0,0,0,1,0,0,1,0,0,1,0,0,1,0,1,1,0,0,0,0,0,1,0,1,1,1,1,1,0,0,1,0,1,0,1,1,0,0,1,0,0,0,1,1,0,0,1,0,1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,1,0,1,0,1,1,1,0,1,1,0,1,1,1,0,0,0,1,1,1,0,0,0,1,0,1,0,1,0,1,0,1,1,1,0,1,1,1,1,1,0,1,1,0,0,1,0,1,1,0,1,1,1,1,0,1,0,0,1,0,1,1,1,0,0,0,1,1,1,1,0,0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,0,0,0,1,0,0,0,0,0,1,0,1,0,0,1,0,1,1,1,1,1,0,0,0,0,0,1,0,0,1,1,0,0,0,1,1,1,0,0,1,1,1,0,1,1,1,0,1,1,1,1,0,0,0,1,0,0,0,0,0,0,0,1,1,1,0,1,1,1,0,1,1,1,1,1,1,0,0,0,0,1,0,1,1,1,1,0,0,1,1,0,1,0,1,1,1,1,1,0,1,0,1,1,0,0,0,0,1,1,0,0,1,0,1,0,1,0,1,1,1,0,0,0,0,0,0,1,0,1,1,1,1,1,0,1,1,0,1,1,1,0,0,0,1,0,1,1,0,1,0,1,1,1,0,0,1,1,1,0,1,1,0,1,0,0,0,1,1,0,0,1,1,1,1,0,1,0,1,0,0,1,0,1,0,0,0,1,1,1,0,1,0,0,1,1,0,0,1,0,1,0,1,0,0,1,0,0,0,0,0,1,1,1,0,0,0,1,1,1,1,0,1,1,1,0,0,0,1,0,0,1,1,1,1,0,0,0,0,1,1,1,1,1,1,1,1,1,0,0,1,1,0,0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,1,1,1,0,0,1,0,1,1,1,1,0,0,0,1,1,1,1,1,0,1,0,1,1,1,1,0,0,0,1,0,0,1,1,0,0,0,1,1,0,0,1,0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,1,0,1,1,0,0,0,1,0,0,0,0,0,1,0,1,0,0,1,1,0,0,0,1,0,0,0,0,0,1,1,0,1,0,1,0,0,0,0,0,0,0,1,1,1,0,0,1,1,0,0,0,1,1,0,0,1,0,0,0,1,0,1,1,1,1,1,0,0,1,1,1,1,1,0,0,1,1,0,1,1,0,1,1,0,1,0,0,0,1,1,0,1,0,1,0,1,0,1,1,0,1,0,1,1,1,1,1,1,1,0,0,0,1,0,0,1,1,0,0,1,0,0,0,0,1,1,0,1,0,0,0,0,0,1,0,1,1,1,1,0,1,0,0,0,1,0,1,1,0,0,1,1,1,1,0,1,0,0,0,1,1,0,1,1,1,0,0,1,1,1,0,1,0,1,1,1,0,1,1,1,0,1,0,0,0,0,1,0,0,1,1,1,1,0,1,0,0,0,0,1,1,0,0,1,0,1,1,1,0,1,0,0,1,0,0,0,1,0,1,1,1,0,0,1,0,0,0,1,0,0,0,1,0,1,0,0,1,0,1,1,0,0,1,1,0,0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,1,1,0,1,0,0,0,1,0,0,0,1,0,1,0,1,0,1,1,1,0,1,0,0,1,1,1,1,1,0,0,1,0,1,1,1,1,1,1,0,0,1,1,0,1,0,1,0,0,1,1,0,1,1,0,0,1,0,0,0,0,1,0,1,1,1,1,1,0,1,1,0,1,0,1,0,0,1,1,0,0,0,0,1,0,1,1,1,0,1,1,0,1,0,1,0,1,1,1,0,1,0,0,0,0,1,0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0,0,0,1,1,1,1,1,1,1,0,1,0,1,1,1,0,0,1,0,1,1,1,1,1,1,1,0,1,1,1,0,0,1,1,1,0,1,0,0,0,1,0,0,1,1,0,0,0,0,1,0,1,0,0,1,1,1,1,0,1,0,1,0,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,1,0,0,0,0,0,1,1,0,0,1,0,0,0,1,1,0,1,1,0,0,0,1,1,1,1,1,1,1,1,1,0,0,1,1,1,0,0,0,1,1,1,0,1,0,1,0,1,0,1,0,1,0,1,0,0,0,0,0,1,0,0,1,0,0,0,1,0,1,1,1,0,0,0,1,0,1,1,0,1,1,0,0,0,1,0,0,0,1,1,1,1,0,1,1,0,0,0,1,0,1,1,0,1,0,0,0,0,0,0,1,0,0,1,1,1,0,0,1,0,1,1,1,1,1,1,0,1,0,1,0,0,1,1,1,0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,1,0,1,0,1,0,1,0,1,0,0,0,1,1,0,0,0,0,0,1,1,1,0,1,1,1,0,1,1,1,1,1,1,0,0,1,0,1,1,1,0,1,1,0,0,1,1,1,1,1,0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,1,1,0,1,1,1,1,1,0,1,1,0,1,0,0,1,1,1,0,0,1,0,0,1,0,0,0,1,0,0,1,0,0,1,0,1,1,1,1,1,1,0,1,1,0,0,0,1,1,1,1,0,0,1,0,1,1,1,0,1,0,1,1,1,1,0,0,0,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1,0,0,0,0,1,1,0,1,0,1,0,1,0,0,0,1,0,1,1,1,0,1,1,1,0,1,0,1,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,0,1,1,0,0,1,0,1,1,0,0,1,1,1,1,1,1,0,0,0,1,0,1,1,0,1,1,0,0,0,0,0,0,1,1,0,1,1,0,1,1,1,0,1,0,0,0,1,1,1,0,1,0,1,0,0,0,1,0,1,1,1,0,0,0,1,0,0,1,0,0,0,1,1,0,1,0,1,1,0,0,1,1,1,0,0,0,0,0,1,0,1,1,1,0,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1,1,1,1,1,0,1,0,1,0,0,1,0,0,1,0,0,0,0,1,0,0,0,1,1,1,1,0,0,1,0,0,1,0,1,0,1,0,0,0,0,0,1,1,0,1,1,0,0,0,1,1,0,0,0,1,0,0,0,0,0,1,1,0,1,1,0,1,1,1,1,0,0,0,0,0,1,1,1,1,1,0,0,0,1,1,1,0,1,0,1,0,1,0,0,1,0,1,0,0,1,0,1,1,0,1,0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,1,1,1,0,0,1,0,1,0,0,0,0,1,1,0,1,1,0,0,1,1,0,0}

Luarea doar a 256 de biți.

Take[Kbin,256]

{1,0,1,0,0,1,0,0,0,1,0,1,1,1,0,1,1,1,0,1,1,1,1,0,0,1,0,1,0,1,1,0,0,0,1,1,1,0,1,1,1,0,0,1,1,0,0,1,0,0,0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,1,1,1,0,1,0,0,1,0,1,1,1,1,0,0,1,0,0,1,0,0,1,0,0,1,1,1,0,1,1,0,1,0,1,0,0,0,1,0,1,0,0,0,1,1,1,0,1,0,0,0,0,1,1,0,1,0,0,0,1,0,1,0,0,0,1,0,0,1,0,1,0,0,1,1,0,0,0,0,0,1,1,1,0,1,0,0,0,0,1,1,1,0,0,1,1,1,1,0,0,1,0,1,0,1,0,0,1,1,0,1,0,0,1,0,0,1,0,0,1,0,0,1,1,0,1,1,0,1,1,1,1,0,1,1,0,1,0,0,0,1,0,0,1,0,0,0,1,1,1,0,0,1,0,0,0,0,0,0,0,0,1,1,0,1,1,0,1,1,0,1,0,1,0,0,1,1,1,1,0,1,1,1,0,0,1,0,0,1,0,1}

Length[Take[Kbin,256]]

256

ELGamal

Messajul.

m10= 22937705806984324019616246073949843906934

22937705806984324019616246073949843906934

Crearea key private și publice pentru Alica și Bob



KeyBobPriv=RandomInteger[p1-2]

912321597388370265196615723725957038873795717071776610944624514794475166318791442334646740799799405881201143608876062634716763225698148125446770563038374661357930239578853480468009324218005238154762408891987759480183792298402164994810756439695790670594057234331851910894131530646370691701993632387335760970968141152210192999277063289652013821147529128266148430967747543343141119213060555701960340937392328652406131508614835094568181041309188604282885552093590332899628780955826652500922626096098349853939901673041164547167928525234971364552371769753345216628134469260013408941991090688897659704286058666064811695027



KeyBobPub=PowerMod[g,KeyBobPriv,p1]

1896983113128795712408841317495968218587562702786715716470114494048614897864097785628957252466854655910477470679027053473392634250751981565459347645266686652938194492797195161305051112846549422640632721253870944513533119141272431598054714543432575129809450214126483325239265129809614014155835123050249640729633430855780098609324785158582139089185603066238368278662318364133747139035108514554895330813928371522387153790283720299346392245909024227176304074343911117903833209487159383764767151351044592904296571458285726232594927714960354540323788088190081413463434361999212230577766615041543587408243503137256030651713



KeyAlicePriv=RandomInteger[p1-2]

2629847483571775950677879892037152520394277775325565832473312957162167496717964828648337769473351978244537450819143765361187540286738503373607535928794317593232618575884594881955014264323062901849065484658093275649522801761453761947679956400408248551026137399205878756806558274366510064038774178882688183733870009327247754651811198000679730677935587657427589823967601039561506936769869238728349061420870750236046795790044983784560840101421055617387170919520259006729176293598222187910608200547625508170677178889641779727541598911790622645793144163960072881548433523509767950611231847568956478479766526622803669603052



KeyAlicePub=PowerMod[g,KeyAlicePriv,p1]

1800559171698314355809769090344284814843308561859957480952343591900856236734839483620928400910046913309327935062505618247234911307849253716257145078202166051819133511964287610343699406384427167099124186296252291354336698437928025280186252217450598309962603494435412054616523645067382935644998015303321995243978670775708181964375386020687488576937831508896655090164553345936660075003415128743757089619135944153248904750265604485889827320490949641065140908918828283662638828991460903639249584297346067864828591959310297543509630608560914533239814218592844451625797683092700353096693019899346167264718451930657005793698

Schimb de key

KmasB=PowerMod[KeyBobPub,KeyAlicePriv,p1]

410653133836123377954119068978689782791287140113143061253825495216444053384827304095877778724377970760443660075689928693649712981400706490235579218337277530340964271673310842689247198929848465466504210337886786839165138036116502530651818587349028948277557272160861193466254757029570118573552160291658537856325191970229365629552686141653009804208472934428503204274920225277467960498439075772504020419884716062460794270987807651749030185801988639446839489245813372249311973229264553275618278137328893691482450062441409926884344109656382569031398237465930268505597566480109031762143491892584428235368139518774712521512

KmasA=PowerMod[KeyAlicePub,KeyBobPriv,p1]

410653133836123377954119068978689782791287140113143061253825495216444053384827304095877778724377970760443660075689928693649712981400706490235579218337277530340964271673310842689247198929848465466504210337886786839165138036116502530651818587349028948277557272160861193466254757029570118573552160291658537856325191970229365629552686141653009804208472934428503204274920225277467960498439075772504020419884716062460794270987807651749030185801988639446839489245813372249311973229264553275618278137328893691482450062441409926884344109656382569031398237465930268505597566480109031762143491892584428235368139518774712521512

Verificarea daca key sunt identice.

KmasB==KmasA

True

Criptam mesajul



MesCripEL=Mod[m10\*KmasB,p1]

1542953686268961035700305366338839185751358083840209524042690483867706381024842171419912358199765582734139953539173632352403502994522271275570049668016371129298901752006909688136015751394742974720502811420674530495814877254460225013665600299613242003499963440662835245536163802675412185640714982512261073014172078230633527191316116707856076281212029077853905139854969836993202603348030782569805634312055626692032442124358189367930284636805863608900503959735141736590512133746094640541314115685252010235765803352315612542212904788420810319389653254808090810815443879559485290624880975655676313993900290213627197036096

Decriptam mesajul



MesDec=Mod[MesCripEL\*ModularInverse[KmasA,p1],p1]

22937705806984324019616246073949843906934

Concluzie:În lucrarea de laborator am elaborat schimbul de chei publice criptarea și decriptarea unui mesaj cu algoritmul RSA,ElGamal.Criptarea asimetrica se folosește și în ziua de azi ca un standart bun.