**Praktikum. RSA**

**OSA I**

**Võtmete genereerimine RSA Algoritmi abil:**

1. Valida kaks algarvu (iga algarv 1024 bits)

Selleks kasuta abiarv 163883276477621298793988904910605723290166320956525233843251082078221554826860024433689882647632816998892075705012569187950205645707586419220007804242104329135461789977770079589898999388384499904533179952206421861902421470990288837164926965819547621284709118665347320906123664523596859809819197903317144512907

lisa sellele oma sünnikuupäev korrutatud 232 (kasutage suurte arvude kalkulaatorit <http://www.mobilefish.com/services/big_number_equation/big_number_equation.php>) Seejärel vali lähim algarv

 <http://www.numberempire.com/primenumbers.php>

Asenda saadud arvust 5 numbrit ja leia veel üks algarv

p (1024bits)= 16388327647762129879398890491060572329016632095652523384325108207822155482686002443368988264763281699889207570501256918795020779

q(1024 bits)= 16388327647762929879398890491660572329016632095652523387325408207822155482686002443363388264763281699889207570501256918795020697

1. Arvutada moodul (kasutage suurte arvude kalkulaatorit <http://www.mobilefish.com/services/big_number_equation/big_number_equation.php> ) n=p×q=

268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522435152722666731703937996071699051480745595304802651904683136512540369629210972814528218322380947821659713051334383988941850062963

1. Arvutada Euleri funktsiooni väärtust

φ(n)=(p-1)(q-1)= 268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522402376067371206644179198290716330336087562040611346857911485996124725318245600809641485945851421258259934636193381475104260021488

1. Valida avatud eksponent *e=* 65537
2. Arvutada salastatud eksponent *d =253274971799702264589470625370798886812362309603648041451518294267671022502223148570511005724318121263023806776141452587862702000916247184684746482246547158725052431749954924745866602126570006201059608051434125345315035100600031108233832179613132559960145*
3. Avalikustada avavõti (e, n)

(65537, 268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522435152722666731703937996071699051480745595304802651904683136512540369629210972814528218322380947821659713051334383988941850062963

)

1. Salvestada privaatvõti (d, n)
2. (*253274971799702264589470625370798886812362309603648041451518294267671022502223148570511005724318121263023806776141452587862702000916247184684746482246547158725052431749954924745866602126570006201059608051434125345315035100600031108233832179613132559960145*

, 268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522435152722666731703937996071699051480745595304802651904683136512540369629210972814528218322380947821659713051334383988941850062963)

**Teksti krüpteerimine RSA abil**

1. Teisenda oma nimi ASCI koodi (<http://www.unit-conversion.info/texttools/ascii/> ):
2. Krüpteeri saadud ASCI kood 101114105107097

Krüpteeritud kujul: 138041004087769493803891758862874039167074381434911966484802224866436647921920695666363713610351244638131737155525137400177656683878421713099334214155754957166913167240081666272995637339471804668188442599897535107962596217304477629826453091586837587474312

**OSA II**

RSA java faili uurimine <http://www.tlu.ee/~matsak/crypto/temp/RSA.java>

Dekrüpteeri RSA programmi abil eelmises osas saadud krüptogramm ja veendu, et on saadud õige algtekst.

Selleks tuleks koodi veidi modifitseerida, et sisestada enda krüptogramm dešifreerimiseks.

**OSA III Miller-Rabin˙i test**

Kasuta abifaili <http://www.tlu.ee/~matsak/crypto/miller_rabin_abifail.pdf> ning näita, et Sinu valitud algarv on tõesti algarv.

**r=log2(arv) Abiks on kalkulaator** [**http://web2.0calc.com/**](http://web2.0calc.com/)

s=

t=1

juhuarv=

**x=juhuarv mod m=**

x2 mod arv

jne