**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)=

q(1024 bits)=

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

φ(n)=(p-1)(q-1)=

1. Valida avatud eksponent *e=*
2. Arvutada salastatud eksponent *d =*
3. Avalikustada avavõti (e, n)
4. Salvestada privaatvõti (d, n)

**Teksti krüpteerimine RSA abil**

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

**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