Eksam, var 5

1. Olgu šifreeritavaks sõnaks *x* ning olemasoleva sammu väljundsõna on 48 bitti Teie matriklinumbrist. Jätkake DES algoritmiga ning arvutage funktsiooni ***f*** = **P**(***S*₁(*B*₁)*S*₂(*B*₂)...*S*₈(*B*₈)**) kasutades S-boxe ja permutatsiooni P:

Permutation P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

2. Näidake alamvõtmete genereerimist algoritmis IDEA lähtudes 128 bitist võtmest *Nimi_Matriklinumber*
3. Näidake algoritmi MARS ühe raundi arvutust (permutatsiooni ilma võtmeta) lähtudes tekstist *Nimi Perekonnanimi Matriklinumber*. (Kasutage esimest 128 bitti)
4. Olgu sõna *x (neli tähte Teie eesnimest)* algoritmi Twofish S-boxide väljund. Jätkake algoritmi sammudega ning arvutage funktsioon *g*.

$$\begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{pmatrix} = M_1 * \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix},$$

M1:

01	EF	5B	5B
5B	EF	EF	01
EF	5B	01	EF
EF	01	EF	5B

Arvutamiseks kasutage korpus 2^8 ning mod $x^8 + x^4 + x^3 + x + 1$

5. Valige oma *perekonnanimest* kolmas ja viimane täht. Teisendage ASCII tabeli abil arvudeks ja võtke lähimad sobivad algarvud. Näidake algoritmi RSA samme lähtudes saadud algarvudest. Pöördväärtuse arvutamiseks kasutage http://www.mtholyoke.edu/~mpeterso/Applets/CalculatorApplet.html
6. Näidake hash-funktsiooni MD5 esimese raundi arvutamist lähtudes järgmistest andmetest:

A = neli viimast tähte eesnimest 16-nd süsteemis
B = neli viimast tähte perekonnanimest 16-nd süsteemis
C = FF DD BB 98
D = 75 53 33 11

Neljanda raundi funktsioon on I(X,Y,Z) =Y⊕(¬Z∨X)

[abcd k s i] a = b + ((a + I(b,c,d) + M[k] + K[i]) <<< s)

[abcd k s i] a = b + ((a + F(b,c,d) + M[k] + K[i]) <<< s)

Sõnaks M on *Tallinna Ylikool*

7. Näidake Hash-funktsiooni SHA-1 abisõnade Wt arvutust lähtudes sellest, et Yq on 512 bitti, mis on võetud järgmisest tekstist:

Minu matriklinumber on XXXX. Minu sünnikuupäev on XXXX. Mina olen informaatika instituudi tudeng.

Arvutage kuni W_{23}.