**Praktikum nr 5. Digitaalne allkiri. RSA+SHA1**

**Võtmete genereerimine RSA Algoritmi abil:**

1. Valida kaks algarvu (iga algarv 1024 bits)

Selleks kasuta abiarv 238564730459694973388537093802694895713859425391881298982

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>

p=

q=

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 ettevalmistamine allkirjastamiseks:**

1. Teisendada oma nimi kahendkoodiks:

|  |
| --- |
|  |

**Hash-funktsioon SHA-1:**

Hash-funktsiooni arvutame tekstist, mis on saadud punktis 8.

1. **Sisendi ühtlustamine** kuni 448 bitti

|  |
| --- |
|  |

1. **Sisendi pikendamine.** Sisendi viimasele kuuekümne neljale kohale (512-448=64) kirjutatakse arvu L (esialgne pikkus) kahendesitus.

|  |
| --- |
|  |

1. Initsialiseerimine:

A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 10325476

E = C3D2E1F0

1. Wt arvutus.

Lähtudes Y0-st moodustage 16 esimest Wt sõna:

|  |  |
| --- | --- |
| W0 |  |
| W1 |  |
| W2 |  |
| W3 |  |
| W4 |  |
| W5 |  |
| W6 |  |
| W7 |  |
| W8 |  |
| W9 |  |
| W10 |  |
| W11 |  |
| W12 |  |
| W13 |  |
| W14 |  |
| W15 |  |

Järgmised 16 sõna arvutatakse: Wt = Wt-16 ⊕ Wt-14 ⊕ Wt-8 ⊕ Wt-3

|  |  |
| --- | --- |
| W16 |  |
| W17 |  |

jne

**Iga raundi operatsiooni võib esitada kui**A, B, C, D, E (CLS5 (A) + ft (B, C, D) + E + Wt + Kt), A, CLS30 (B), C, D



1. Arvutame CLS5 (A) :

|  |
| --- |
|  |

1. Arvutame esimese raundi jaoks ft (B, C, D)= (B & C) ∨ (¬ B & D):

|  |
| --- |
|  |

1. Arvutame saadut tulemuste abil: (CLS5 (A) + ft (B, C, D) + E + W0 + K0), siin
0 ≤ t ≤ 19 Kt = 5A827999
2. Uus A võrdub eelmises punktis saadud tulemusega
3. Uus B= vana A:

|  |
| --- |
|  |

1. Uus C = CLS30 (vana B):

|  |
| --- |
|  |

1. Uus D = vana C:

|  |
| --- |
|  |

1. Uus E = vana D
2. Olgu uus ABCD- hash-funktsiooni lõppväljund (reaalselt oleks vaja läbida 80 kodeerimisringi). Kasutades RSA ja privaatvõtit krüpteerime saadud koodi P(M)=Memod *n=*