**Praktikum. Digitaalne allkiri. RSA+SHA2**

**OSA I**

**Võtmete genereerimine RSA Algoritmi abil:**

1. RSA praktikumis on genereeritud võtmed. Koopeeri siia vajalikud andmed:

Avalik võti (e, n) (65537, 268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522435152722666731703937996071699051480745595304802651904683136512540369629210972814528218322380947821659713051334383988941850062963

)

Privaatvõti (d, n)

1. (*253274971799702264589470625370798886812362309603648041451518294267671022502223148570511005724318121263023806776141452587862702000916247184684746482246547158725052431749954924745866602126570006201059608051434125345315035100600031108233832179613132559960145*

, 268577283090417735618014277218355850768114633342949075168004052415260679930233135735572379692808386538109658506674148152205522435152722666731703937996071699051480745595304802651904683136512540369629210972814528218322380947821659713051334383988941850062963)

<http://www.mobilefish.com/services/big_number_equation/big_number_equation.php>)

**Teksti ettevalmistamine allkirjastamiseks:**

1. Teisendada oma nimi kahendkoodiks:

|  |
| --- |
| erika |

**Hash-funktsioon SHA-1:**

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

1. **Sisendi ühtlustamine** kuni 448 bitti

|  |
| --- |
| 0110010101110010011010010110101101100001100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 |

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

|  |
| --- |
| 01100101011100100110100101101011011000011000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000101000 |

1. Initsialiseerimine:

A := 0x6a09e667

B := 0xbb67ae85

C := 0x3c6ef372

D := 0xa54ff53a

E := 0x510e527f

F := 0x9b05688c

G := 0x1f83d9ab

H := 0x5be0cd19

1. Wt arvutus.

Lähtudes Y0-st moodustage 16 esimest Wt sõna:

|  |  |
| --- | --- |
| W0 | 01100101011100100110100101101011 |
| W1 | 01100001100000000000000000000000 |
| W2 | 00000000000000000000000000000000 |
| W3 | 00000000000000000000000000000000 |
| W4 | 00000000000000000000000000000000 |
| W5 | 00000000000000000000000000000000 |
| W6 | 00000000000000000000000000000000 |
| W7 | 00000000000000000000000000000000 |
| W8 | 00000000000000000000000000000000 |
| W9 | 00000000000000000000000000000000 |
| W10 | 00000000000000000000000000000000 |
| W11 | 00000000000000000000000000000000 |
| W12 | 00000000000000000000000000000000 |
| W13 | 00000000000000000000000000000000 |
| W14 | 00000000000000000000000000000000 |
| W15 | 00000000000000000000000000101000 |

Järgmised 16 sõna arvutatakse: Wt = σ1(Wt-2)+ Wt-7+σ0(Wt-15)+ Wt-16

<http://www.utdallas.edu/~dodge/EE2310/lec14.pdf>

righSHIFT(3): 10101010🡪00010101

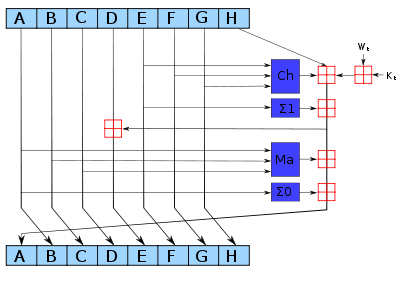
σ0 := (w[i-15] rightrotate 7) ⊕ (w[i-15] rightrotate 18) ⊕ (w[i-15] rightshift 3)

σ1 := (w[i-2] rightrotate 17) ⊕ (w[i-2] rightrotate 19) ⊕ (w[i-2] rightshift 10)

01100001100000000000000000000000

|  |  |
| --- | --- |
| W16 | [00000000000000000000000000000000 ⊕ 00000000000000000000000000000000 ⊕ 00000000000000000000000000000000] + 00000000000000000000000000000000+ [00000000110000110000000000000000 ⊕ 00000000000000000001100001100000 ⊕ 00001100001100000000000000000000] + 01100101011100100110100101101011=  =1100111100110001100001100000+  01100101011100100110100101101011=  01110010011001011000000111001011  !!!! Kas on 32 bitti? |
| W17 |  |

jne

**Iga raundi võib esitada kui**

1. Arvutame Ch:

\operatorname{Ch}(E,F,G) = (E \and F) \oplus (\neg E \and G)

E := 0x510e527f

F := 0x9b05688c

G := 0x1f83d9ab

!!!!!! DWORD

|  |
| --- |
| (0x510e527f & 0x9b05688c) ⊕ (¬0x510e527f & 0x1f83d9ab)= 1104400C ⊕ E818980 =1F85C98C=00011111100001011100100110001100  !!! kontrolli kas on 32 bitti!! |

1. Arvutame Σ1

\Sigma_1(E) = (E\!\ggg\!6) \oplus (E\!\ggg\!11) \oplus (E\!\ggg\!25)

|  |
| --- |
| 0x510e527f=01010001000011100101001001111111  11111101010001000011100101001001 ⊕ 01001111111010100010000111001010 ⊕ 01010001000011100101001001111111 =00110101100001110010011100101011 |

Konstandid k[0..63] :=

0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,

0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,

0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,

0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,

0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,

0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,

0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,

0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2

1. Arvutame Wt +Kt =W0+K0

|  |
| --- |
| 01100101011100100110100101101011+1000010100010100010111110011000=10100111111111001001100100000011 |

1. Arvutame saadut tulemuste abil vahemuutuja X1= [H+( Wt +Kt)+Ch+Σ1] mod 232

|  |
| --- |
| 0x5be0cd19=1011011111000001100110100011001  1011011111000001100110100011001+10100111111111001001100100000011+ 00011111100001011100100110001100 + 00110101100001110010011100101011=  01011000111010100101011011010011 |

1. Arvutame Ma

\operatorname{Ma}(A,B,C) = (A \and B) \oplus (A \and C) \oplus (B \and C)

A := 0x6a09e667

B := 0xbb67ae85

C := 0x3c6ef372

|  |
| --- |
| (0x6a09e667 & 0xbb67ae85) ⊕ (0x6a09e667 & 0x3c6ef372)⊕ (0xbb67ae85 & 0x3c6ef372)= 2A01A605 ⊕ 2808E262 ⊕ 3866A200=3A6FE667=00111010011011111110011001100111 |

1. Arvutame Σ0

\Sigma_0(A) = (A\!\ggg\!2) \oplus (A\!\ggg\!13) \oplus (A\!\ggg\!22)

|  |
| --- |
| 0x6a09e667=01101010000010011110011001100111  11011010100000100111100110011001 ⊕ 00110011001110110101000001001111 ⊕ 00100111100110011001110110101000=11001110001000001011010001111110 |

1. Uus A=X1 +Σ0 mod 232

|  |
| --- |
| 01011000111010100101011011010011+11001110001000001011010001111110  = 00100111000010110000101101010001 |

1. Uus B = vana A:

|  |
| --- |
| 01101010000010011110011001100111 |

1. Uus C = vana B:

|  |
| --- |
| 0xbb67ae85=10111011011001111010111010000101 |

1. Uus D = vana C

|  |
| --- |
| 00111100011011101111001101110010 |

1. Uus E=vana D + X1 mod 232:

|  |
| --- |
| 0xa54ff53a =10100101010011111111010100111010  10100101010011111111010100111010 +01011000111010100101011011010011=  11111110001110100100110000001101 |

1. Uus F=vana E:

|  |
| --- |
| 0x510e527f=01010001000011100101001001111111 |

1. Uus G=vana F:

|  |
| --- |
| 0x9b05688c=10011011000001010110100010001100 |

1. Uus H=vana G:

|  |
| --- |
| 0x1f83d9ab=00011111100000111101100110101011 |

1. Olgu uus ABCDEFGH- hash-funktsiooni lõppväljund (reaalselt oleks vaja läbida 64 kodeerimisringi). Kasutades RSA ja privaatvõtit krüpteerime saadud koodi

M=0010011100001011000010110101000101101010000010011110011001100111101110110110011110101110100001010011110001101110111100110111001011111110001110100100110000001101010100010000111001010010011111111001101100000101011010001000110000011111100000111101100110101011

Kasutan suurte arvu kalkulaatorit ja funktsiooni powMod(a,b,c)

P(M)=Memod *n= 236428145259807023167111525960845767013153851542228149673756105200042858722981286252349881146673211721887956527513781725396904679171595504876048792782791110696514199126080306574024571499585175477800405337607852991223478800829070925832916318393395109220645*

!!! See vastus on kümnendarv

Cdmod*n*=17659714526592621658596393880602558995183531341946615046371803147056848296363 (kümnendarv)= 10011100001011000010110101000101101010000010011110011001100111101110110110011110101110100001010011110001101110111100110111001011111110001110100100110000001101010100010000111001010010011111111001101100000101011010001000110000011111100000111101100110101011