**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)

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

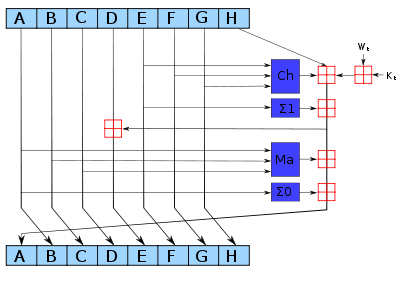
Järgmised 16 sõna arvutatakse: Wt = σ1(Wt-2)+ Wt-7+σ0(Wt-15)+ Wt-16

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)

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

jne

**Iga raundi võib esitada kui**

1. Arvutame Ch:

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

|  |
| --- |
|  |

1. Arvutame Σ1

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

1. Arvutame Ma

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

|  |
| --- |
|  |

1. Arvutame Σ0

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

|  |
| --- |
|  |

1. Uus A=X1 +Σ0 mod 232

|  |
| --- |
|  |

1. Uus B = vana A:

|  |
| --- |
|  |

1. Uus C = vana B:

|  |
| --- |
|  |

1. Uus D = vana C

|  |
| --- |
|  |

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

|  |
| --- |
|  |

1. Uus F=vana E:

|  |
| --- |
|  |

1. Uus G=vana F:

|  |
| --- |
|  |

1. Uus H=vana G:

|  |
| --- |
|  |

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