**Praktikum nr 4. Hash-funktsioonid**

**MD5**

1. **Olgu sisendiks Sinu eesnimi + perekonnanimi, täida järgmine tabel, jättes vahele üleliigsed lahtrid:**

**Nimi:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **e** | **r** | **i** | **k** | **a** | **m** | **a** | **t** | **s** |
| **a** | **k** |  |  |  |  |  |  |  |

Nimi kahendkoodis (Konvertimisel on abiks <http://www.home2.paulschou.net/tools/xlate/> ):

|  |
| --- |
| 01100101 01110010 01101001 01101011 01100001 01101101 01100001 01110100 01110011 01100001 01101011 00001101 00001010 00100000 |

|  |
| --- |
|  |

Vastavalt saadud kahendkoodi pikkusele saab kirja panna, et sisendi pikkus L=

1. **Sisendi ühtlustamine (kuni 448 bitti):**

|  |
| --- |
| 0110010101110010011010010110101101100001011011010110000101110100011100110110000101101011000011010000101000100000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 |

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

|  |
| --- |
| 01100101011100100110100101101011011000010110110101100001011101000111001101100001011010110000110100001010001000001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001110000 |

1. **Esimese raundi arvutus**. **Ettevalmistus.** Initsialiseerimisvektor ABCD on:

А = 01 23 45 67 =00000001 00100011 01000101 01100111

В = 89 AB CD EF = 10001001 10101011 11001101 11101111

С = FE DC BA 98 = 11111110 11011100 10111010 10011000

D = 76 54 32 10= 01110110 01010100 00110010 00010000

1 raundi funktsioon: F(X,Y,Z)=(X&Y)∨(¬X&Z)

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

*k*=0, *i*=1, *s* väärtused esimeses raundis on: 7, 12, 17, 22, ehk esimene nendest on 7

plokk krüpteerimiseks (Sinu nime 4 esimest tähte) nr i paigutatakse massiivi M:

täpsustame: [abcd **0 7 1**] a =b + ((a + F(b,c,d) + M[**0**] + K[1]) <<< **7**)

*K0=K*[*1*] = *int*(4294967296 \*|*sin*(***i***)| ) = *int*(4294967296 \*|*sin*(***1***)| ), kus i on **radiaanides**.

|  |
| --- |
| 3614090360 |

ning kahendkoodis:

|  |
| --- |
| 11010111011010101010010001111000 |

M[0] (neli esimest tähte sinu nimest):

|  |
| --- |
| 01100101011100100110100101101011 |

1. **Esimese raundi arvutus**. **F funktsiooni arvutus**

**F(x,y,Z) 🡪 F(B, C, D)**

Antud juhul X=b, Y=c, Z=d !!!!! Paneme kalkulaatoris DWORD sisse

(X&Y)∨(¬X&Z)= (B&C)∨(¬B&D)=

|  |
| --- |
| 10001000100010001000100010001000∨1110110010101000011001000010000 1110110010101000011001000010000=11111110110111001011101010011000 |

1. **Esimese raundi arvutus**. **[ABCD 0 7 1]**

a =b + ((a + F(b,c,d) + M[**0**] + K[1]) <<< **7**)

a:

|  |
| --- |
| 00000001 00100011 01000101 01100111 |

a**+F(b,c, d)**:

|  |
| --- |
| 11111111111111111111111111111111  |

a+F(b,c, d)**+ M[0]**:

|  |
| --- |
| 101100101011100100110100101101010 |

a+F(b,c, d)+ M[0]+ **K[1]**:

|  |
| --- |
| 1000111100110111010000110111100010 |

!!!!!!!!!! kas on 32 bitti

Mod 232=4294967296=100000000000000000000000000000000

(a+F(b,c, d)+ M[0]+ K[1]) <<< **7**:

|  |
| --- |
| 0011110011011101000011011110001001101110100001101111000100011110 |

**b +** ((a + F(b,c,d) + M[**0**] + K[1]) <<< **7**):

A=11111000001100101011111100001101

Kas on 32 bitti ?!!!

1. **Esimese raundi arvutus**. **Ettevalmistus.** **[DABC 1 12 2]**.

**D on vektorist (vana)**

**A on meie eelmise ringi tulemus**

**B ja C on vektorist (vana)**

d =a + ((c + F(a,b,c) + M[**1**] + K[2]) <<< **2**)

*K*[*2*] = *int*(4294967296 \*|*sin*(*2*)| ) =

|  |
| --- |
| 3905402710 |

ning kahendkoodis:

|  |
| --- |
| 11101000110001111011011101010110 |

M[1]:

|  |
| --- |
| 01100001011011010110000101110100 |

1. **Esimese raundi arvutus**. **F funktsiooni arvutus. [DABC 1 12 2]**.

F(x,y,z) 🡪F(a,b,c)

Antud juhul X=a, Y=b, Z=c

(X&Y)∨(¬X&Z)= (A&B)∨(¬A&C)=

!!!!!!!!!!!!! DWORD

|  |
| --- |
| 10001000001000101000110100001101∨(111110011010100000011110010&11111110 11011100 10111010 10011000)= 10001110111011101000110110011101 |

1. **Esimese raundi arvutus**. **[DABC 1 12 2]**.

d =a + ((c + F(a,b,c) + M[**1**] + K[2]) <<< **2**)

c:

|  |
| --- |
| 11111110 11011100 10111010 10011000 |

c**+F(a,b, c)**:

|  |
| --- |
| 110001101110010110100100000110101 |

c+F(a,b, c)**+ M[1]**:

|  |
| --- |
| 111101111001110001010100110101001 |

c+F(a,b, c)+ M[1]+ **K[2]**:

|  |
| --- |
| 1011011000000000000110000011111111 mod 100000000000000000000000000000000= |

!!!!!!!!!!!!!!!!!!!!!!!!!! 32 bitti

 (c+F(a,b, c)+ M[1]+ K[2]) <<< **12**:

|  |
| --- |
| 1101100000000000011000001111111100000110000011111111110110000000 |

**a +** ((c + F(a,b,c) + M[**1**] + K[2]) <<< **12**):

Kas on 32 bitt!!!

|  |
| --- |
| 11111110010000101011110010001101 |

Kirjelda, mis muutub kolmandas ringis, kuidas näeks välja funktsioon, millised muutujad tulevad kasutusele ja mis järjekorras.