**Praktikum nr 4. Hash-funktsioonid**

**MD5**

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

**Nimi:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

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

|  |
| --- |
|  |

|  |
| --- |
|  |

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

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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**)

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

|  |
| --- |
|  |

ning kahendkoodis:

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

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

(X&Y)∨(¬X&Z)=

|  |
| --- |
|  |

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

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

a:

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

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

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

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

|  |
| --- |
|  |

ning kahendkoodis:

|  |
| --- |
|  |

M[1]:

|  |
| --- |
|  |

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

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

(X&Y)∨(¬X&Z)=

|  |
| --- |
|  |

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

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

c:

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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