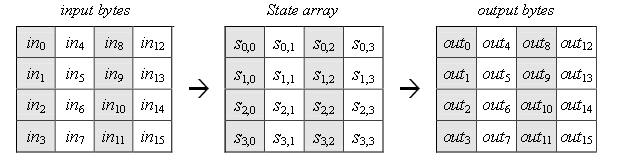
**Praktikum. Algoritm AES**

****

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Kasutades oma nime ees ja perekonnanime tähti täida ruut avateksti jaoks.**  |  |  |  |  | | --- | --- | --- | --- | | e | a | s | r | | r | m | a | i | | i | a | k | k | | k | t | e | a | | 1. **Kasutades oma tänava ja/või linna tähti täida ruut krüpteerimisvõtme jaoks**  |  |  |  |  | | --- | --- | --- | --- | | i | n | l | d | | l | d | m | u | | m | u | a | i | | a | i | n | l | |
| 1. **Avatekst 16-nd süsteemis**  |  |  |  |  | | --- | --- | --- | --- | | 65 | 61 | 73 | 72 | | 72 | 6d | 61 | 69 | | 69 | 61 | 6b | 6b | | 6b | 74 | 65 | 61 | | 1. **Võti 16-nd süstemis**  |  |  |  |  | | --- | --- | --- | --- | | 69 | 6e | 6c | 64 | | 6c | 64 | 6d | 75 | | 6d | 75 | 61 | 69 | | 61 | 69 | 6e | 6c | |

1. **Järgnevalt genereerige esimese kahe raundi jaoks alamvõtmeid kasutades KeyExpansion.**

Esimest neli elementi täitke oma krüpteerimisvõtme osadega (Iga osa 4 Baidi)

Konvertimise abiks on <http://home2.paulschou.net/tools/xlate/>



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| W0: | 69 | 6c | 6d | 61 |
| W1: | 6e | 64 | 75 | 69 |
| W2: | 6c | 6d | 61 | 6e |
| W3: | 64 | 75 | 69 | 6c |

Nk=4

R=10 raundi

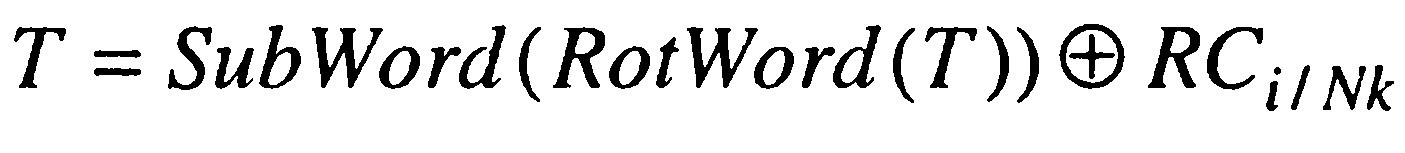
Suurim indeks alamvõtme jaoks : (4\*(R+1)-1)=(4\*(10+1)-1)=43

W4 jaoks on n=4, kordne Nk-le

Teostage teisendust

T: T=Wi-1

|  |  |  |  |
| --- | --- | --- | --- |
| 64 | 75 | 69 | 6c |



**RotWord** nihutab (keerab, ehk > >) sisendsõna 1 Baidi võrra (8 bitt) vasakule

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T=RotWord(T) | 75 | 69 | 6c | **64** |

**SubWord** teostab iga Baidiga teisendust tabeli abil, mis on sama mis protseduuris SubBytes (vaata p.7)

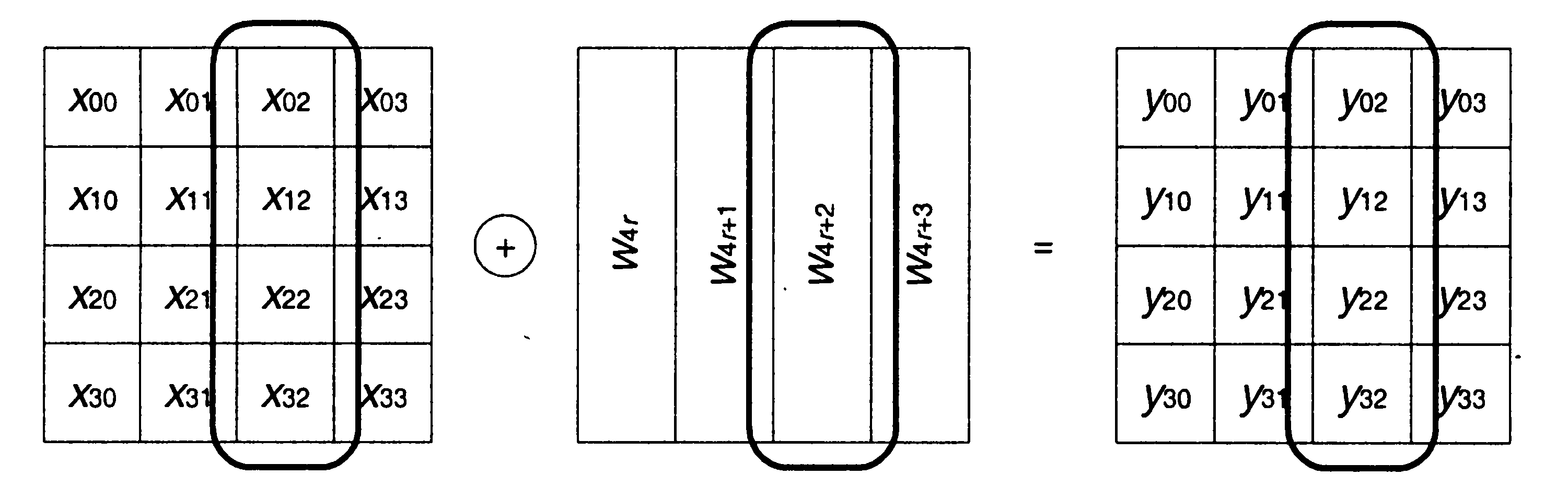
RCi/Nk kujutab endast sõnu, kus kõik Baidid peale esimest on nullid, ning esimene Bait on 2n-1 mod 256, kus n=i/Nk

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T=SubWord(T) 16-nd süsteemis   |  |  |  |  | | --- | --- | --- | --- | | 9D | F9 | 50 | 9F | | Ci HEX kujul   |  |  |  |  | | --- | --- | --- | --- | | 0 | 0 | 0 | 1 | |
| T⊕Ci   |  |  |  |  |  | | --- | --- | --- | --- | --- | | T | 9D | F9 | 50 | 9F | | Ci | 0 | 0 | 0 | 1 | | Tuus | 9D | F9 | 50 | 9E | | |
| W4=:W4-4⊕T= W0⊕T   |  |  |  |  |  | | --- | --- | --- | --- | --- | | W0 | 69 | 6c | 6d | 61 | | Tuus | 9D | F9 | 50 | 9E | | W4 | F4 | 95 | 3D | FF | | |
| Järgmise W5 arvutamiseks vajame T: T=Wi-1=W4  Antud juhul *i* ei ole kordne Nk-le ning ei ole Nk =8 või (i mod Nk)=4 | |
| W5=:W5-4⊕T= W1⊕T   |  |  |  |  |  | | --- | --- | --- | --- | --- | | W1 | 6e | 64 | 75 | 69 | | T | F4 | 95 | 3D | FF | | W5 | 9A | F1 | 48 | 96 | | |
| T=Wi-1=W5, *i* ei ole kordne Nk-le ning ei ole Nk =8 või (i mod Nk)=4  W6=:W6-4⊕T= W2⊕T   |  |  |  |  |  | | --- | --- | --- | --- | --- | | W2 | 6c | 6d | 61 | 6e | | T | 9A | F1 | 48 | 96 | | W6 | F6 | 9C | 29 | F8 |  |  |  |  |  |  | | --- | --- | --- | --- | --- | | W3 | 64 | 75 | 69 | 6c | | T | F6 | 9C | 29 | F8 | | W7 | 92 | E9 | 40 | 94 | | |

16-nd süsteemis:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| W4: | F4 | 95 | 3D | FF |
| W5: | 9A | F1 | 48 | 96 |
| W6: | F6 | 9C | 29 | F8 |
| W7: | 92 | E9 | 40 | 94 |

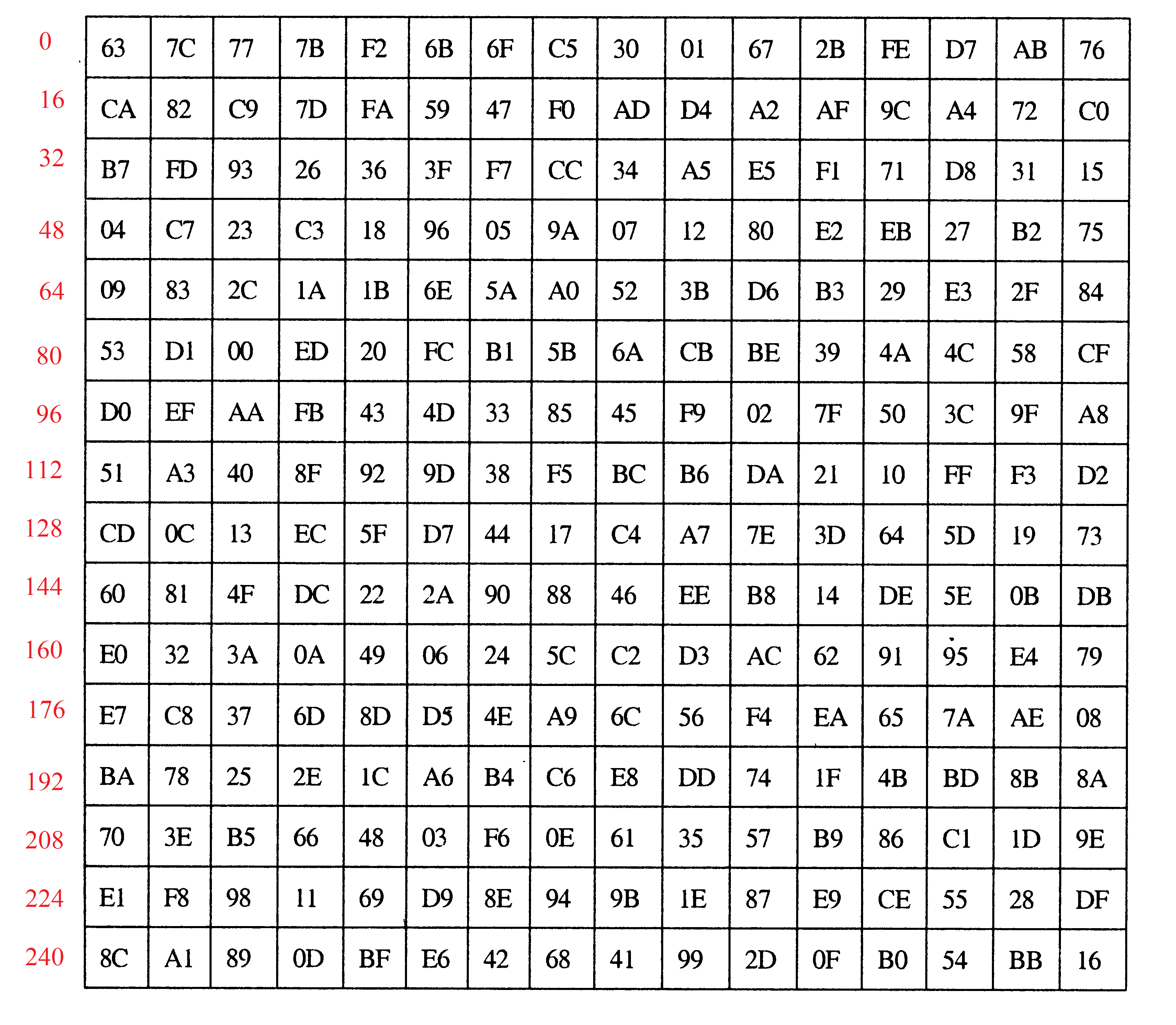
1. **Lisage alamvõtmed W4..W7 kasutades AddRoundKey**

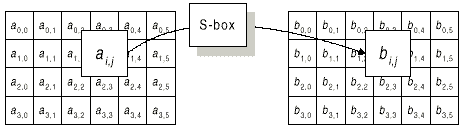


Selles punktis kasutage XOR arvutamiseks kalkulaatorit

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x:   |  |  |  |  | | --- | --- | --- | --- | | 65 | 61 | 73 | 72 | | 72 | 6d | 61 | 69 | | 69 | 61 | 6b | 6b | | 6b | 74 | 65 | 61 | | W:  W4 W5 W6 W7   |  |  |  |  | | --- | --- | --- | --- | | F4 | 9A | F6 | 92 | | 95 | F1 | 9C | E9 | | 3D | 48 | 29 | 40 | | FF | 96 | F8 | 94 | | y:   |  |  |  |  | | --- | --- | --- | --- | | 91 | FB | 85 | E0 | | E7 | 9C | FD | 80 | | 54 | 29 | 42 | 2B | | 94 | E2 | 9D | F5 | |

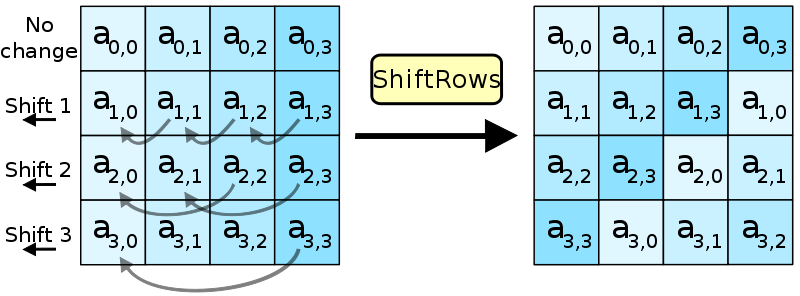
1. **Alustatakse raundidega. SubByte protseduuri teostame S-boxi abil**





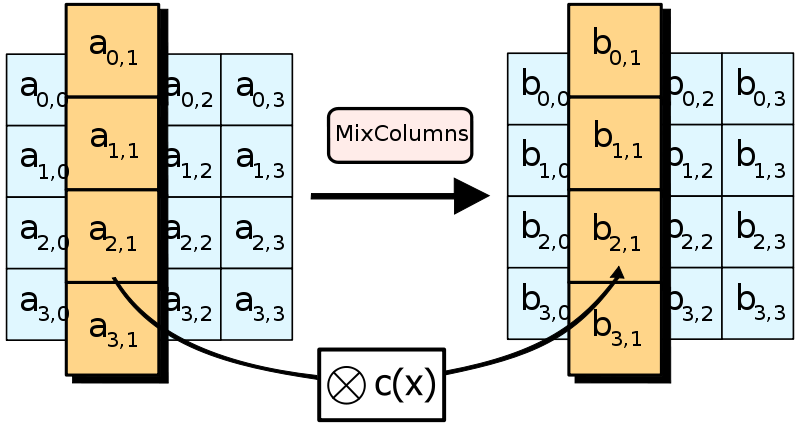
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ai:   |  |  |  |  | | --- | --- | --- | --- | | 91 | FB | 85 | E0 | | E7 | 9C | FD | 80 | | 54 | 29 | 42 | 2B | | 94 | E2 | 9D | F5 | | Tulemus (bi)   |  |  |  |  | | --- | --- | --- | --- | | 81 | 0F | D7 | E1 | | 94 | DE | 54 | CD | | 20 | A5 | 2C | F1 | | 22 | 98 | 5E | E6 | |

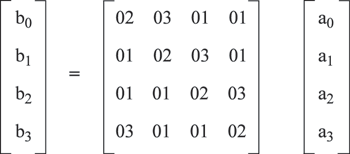
1. **ShiftRows. Esimene rida jääb muutmatul kujul. Teise rea nihutatud Baitide arv on 1, kolmanda – 2, neljanda – 3.**



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ai:   |  |  |  |  | | --- | --- | --- | --- | | 81 | 0F | D7 | E1 | | 94 | DE | 54 | CD | | 20 | A5 | 2C | F1 | | 22 | 98 | 5E | E6 | | Tulemus   |  |  |  |  | | --- | --- | --- | --- | | 81 | 0F | D7 | E1 | | DE | 54 | CD | 94 | | 2C | F1 | 20 | A5 | | E6 | 22 | 98 | 5E | |

1. **MixColumns. Teostage korrutamist GF(28) korpuse siseselt.**





XOR teostamiseks kasutage kalkulaatorit

B0=RIDA korda TULP=02xA0 xor 03xA1 xor 01xA2 xor 01xA3

B1=RIDA korda TULP=01xA0 xor 02xA1 xor 03xA2 xor 01xA3

B2=RIDA korda TULP=01xA0 xor 01xA1 xor 02xA2 xor 03xA3

B3=RIDA korda TULP=03xA0 xor 01xA1 xor 01xA2 xor 02xA3

B0=02xA0,1mod x8+ x4+ x3+x+1=02x81mod x8+ x4+ x3+x+1=102mod x8+ x4+ x3+x+1= 100000010mod100011011=**11001**

Remainder: **11001**

XOR

03xA0,1mod100011011=03xDE mod100011011=29Amod100011011=1010011010 mod100011011=**10101100=AC**

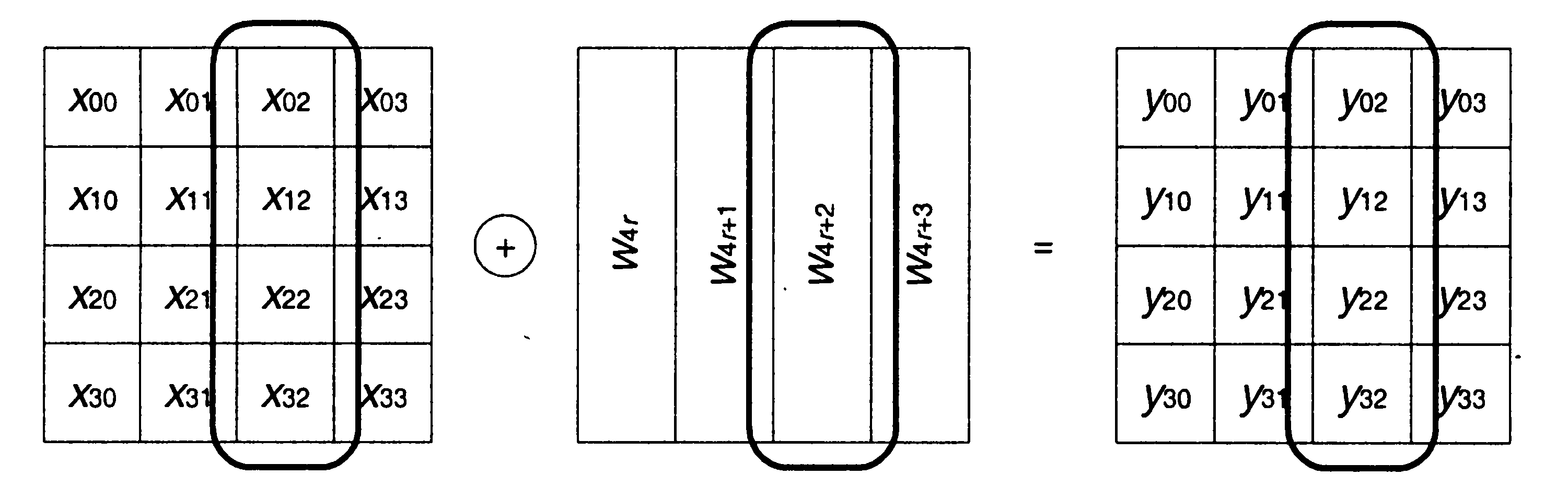
Remainder: **10101100**

……

B0=19 xor AC xor …. Xor …

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ai:   |  |  |  |  | | --- | --- | --- | --- | | 81 | 0F | D7 | E1 | | DE | 54 | CD | 94 | | 2C | F1 | 20 | A5 | | E6 | 22 | 98 | 5E | | Tulemus   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |

1. **Lisage alamvõtmed W4..W7 kasutades AddRoundKey**



Selles punktis kasutage XOR arvutamiseks kalkulaatorit

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x:   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | W:  W4 W5 W6 W7   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | y:   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |

Esimene raund on läbitud