Algoritm MARS,
permutatsioon ilma võtmeta

11001100101010101001001010011010	10101010100100101001001010011010	10010010110011001010101001011010	10011010110011001010101001011010
		S-box tulemus: 11010011100111111011000100011001	10011010110011001010101010011010
		Xor: 10000010101001100011011100000011	
			10011010100110101100110010101010
		S-box tulemus:	
		liitmine (mod 2^{32})	

Algoritm MARS,
alamvõtmete genereerimine

Olgu võtmeks 128 bitti (ehk 4 korda 32): 11001100 10101010 10010010 10011010 10010010 11001100 10101010 10011010 10010010 10011010 10010010 11001100 10101010 10010010 10011010 10010010

T0=10101010 10010010 10011010 10010010

T1=10010010 10011010 10010010 11001100

T2=10010010 11001100 10101010 10011010

T3=11001100 10101010 10010010 10011010

T4=n=4

T5=T6=T7=T8=T9=T10=T11=T12=T13=T14=0

Lineaarne teisendus:

for (j=0 ; j<4; j++) {

for (i=0; i< 14; i++){

$T_i = T_i \oplus ((T_{i-7 \bmod 15} \oplus T_{i-2 \bmod 15}) <<< 3) \oplus (4i + j)$

}}

$T0=T0 \oplus [(T_{0-7 \bmod 15} \oplus T_{0-2 \bmod 15}) <<< 3] \oplus (4*0 + 0)=T0 \oplus [(T8 \oplus T13) <<< 3] \oplus 0=$

= 10101010 10010010 10011010 10010010 ⊕ [(00000000 00000000 00000000 00000000 ⊕ 00000000 00000000 00000000 00000000) <<< 3] ⊕ 00000000 00000000 00000000 00000000 =

= 10101010 10010010 10011010 10010010 ⊕ (00000000 00000000 00000000 00000000 <<< 3) ⊕ 00000000 00000000 00000000 00000000 =

= 10101010 10010010 10011010 10010010 ⊕ 00000000 00000000 00000000 00000000=10101010 10010010 10011010 10010010

Korratakse iga T jaoks 4 korda

Kui on valmis, siis
Massiivi T permutatsioon:

```
for (j=0 ; j<4; j++) {
        for (i=0; i< 14; i++){
                T_i = (T_i ⊕ S(low 9 bit of T_{i-1 mod 15})) <<< 9
}}
```

Näiteks

Olgu T0=10101010 10010010 10011010 10010010 ja T1= 11110011 10101011 11000011 10101111

Ning olgu arvutamisel T1

T1=[T1⊕S(0 10010010)] <<< 9=[11110011 10101011 11000011 10101111⊕10110011 00100010 01010001 01111110] <<< 9 =

=01000000 10001001 10010010 11010001 = 00010011 00100101 10100010 10000001

Korratakse iga T jaoks 4 korda

Valitakse 10 elementi ja paigutatakse uude, laiendatud võtmete massiivi

```
for (j=0 ; j<4; j++) {
                for (n=0; n< 10; n++){
                        k_{10j+n} = T_{4n mod15}
```

}}

$K0=T_{4*0 \bmod 15}=T0$

$K1=T_{4*1 \bmod 15}=T4$

$K2=T_{4*2 \bmod 15}=T8$

$K3=T_{4*3 \bmod 15}=T12$

$K4=T_{4*4 \bmod 15}=T1$

$K5=T_{4*5 \bmod 15}=T4$

Jne

Alamvõtmete kontroll

- Kaks esimest bitti alamvõtmest asendada väärtusega “1”. Vana väärtus salvestada muutujasse *j*. Tähistada uus alamvõti tervikuna sümboliga *W*.

Olgu K0=10101010 10010010 10010000 00000010

W0=10101010 10010010 10010000 00000011

J= 10101010 10010010 10010000 00000010

Mask= 00000000 00000000 00001111 11111100 i on biti koht maskis , Wi on väärtus kohal i

– Nullida need bitid, mida *maskis M tähistab arv* 1 ja mis seejuures vastavad ühele järgmistest tingimustest:
  i<2; i=31; $W_i \neq W_{i-1}$; $W_i \neq W_{i+1}$;

Mask= 00000000 00000000 00000111 11111000

- Kasutatakse korrigeerivaid arve B (S boxi väärtused 265, 266, 267, 268), ehk B_0=a4a8d57b, B_1=5b5d193b, B_2=c8a8309b, B_3=73f9a978. Viimasena tuleb arvutada lõplikud alamvõtmed:

$K_i=W \oplus ((B_j <<< \text{low 5 bitt } (K_{i-1})) \& M)$, kus j = J & 0x00000003=10101010 10010010 10010000 00000010 & 00000000 00000000 00000000 00000011=

00000000 00000000 00000000 00000010= kümnendarv on 2

Algoritm MARS, permutatsioon E

I=11100101 10101111 10010011 11100001

O2=I=11100101 10101111 10010011 11100001

O3=$\mathbf{O_2}$ **<<< 13=**111 10010011 11100001 11100101 10101

$\mathbf{O_2 = O_2 + k_{2*0+4} \bmod 2^{32}}$ = 11110010 01111100 00111100 10110101 + 00010011 00100101 10100010 10000001 $\mathbf{\bmod 2^{32}}$ =

=10000010110100001110111110011011O mod 10000000000000000000000000000000 = 00000101 10100001 11011111 00110110

$$O_3 = O_3 * k_{2r+5} \bmod 2^{32}$$