ISSN 2181-3187

KALITLAR GENERATSIYASI ALGORITMI (KEY SCHEDULE)

Jo'rayev Sirojbek O'rol o'g'li, 1993-yil 06-dekabr
Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti
"Amaliy matematika va intellektual texnologiyalar" fakulteti
"Axborot xavfsizligi" yo`nalishi 2-bosqich magistranti.
sirojbekjorayev1@gmail.com, +998996771593

Annotatsiya: Dastlabki kalitni kengaytirishda, avval 128 bitli (16 bayt, simvol) boshlang'ich kiruvchi kalit kiritib olinadi va to'rtta (w1, w2, w3, w4) 32 bitdan iborat bo'lakka bo'linadi. Qolgan kengaytirilgan kalitlar mana shu to'rtta (w1, w2, w3, w4) kengaytirilgan kalitlar yordamida topiladi.

Kalit so'zlar: Raund kalitlari, raund soni, Dastlabki kalit.

Raund kalitlari daslabki kalitdan, algoritmda ko'zda tutilgan hamma raundlar uchun yaratib olinadi. Bu jarayon:

-kalitni kengaytirish (Key Expansion);

-raund kalitlarini tanlash (Round Key Selection);

bosqichlaridan iborat.

Raund kalitlarining umumiy bitlari soni kirish ma'lumotining bitlari sonining raund soniga ko'paytmasiga va yana bitta kirish ma'lumoti bitlari sonini yig'indisiga teng (misol uchun 128 bitli shifrlash uchun 128*10+128=1408 bit raund kaliti kerak bo'ladi), ya'ni N_b (N_{r+1}) va l (N)=128*11=1408 bit.

Demak, 128 bit uzunlikdagi blok va 10 raund uchun 1408 bit raund kalitlari talab qilinadi. Dastlabki kalitni kengaytirishda, avval 128 bitli (16 bayt, simvol) boshlang'ich kiruvchi kalit kiritib olinadi va to'rtta (w1, w2, w3, w4) 32 bitdan iborat bo'lakka bo'linadi. Qolgan kengaytirilgan kalitlar mana shu to'rtta (w1, w2, w3, w4) kengaytirilgan kalitlar yordamida topiladi. Kengaytirilgan kalitlar soni

$N[w(i)] = N_b (N_{r+1})$;

Biz ko'rayotgan holatda $N_b = 4$, $N_r= 10$ ga teng ya'ni, bayt uzunligi 4 ga, raundlar soni 10 ga teng. Shularni bilgan holda N[w(i)] ni topiladi:

N[w(i)]= 4*(10+1) = 44

Demak, 128 bitli kirish blokiga va 10 ta raundga ega bo'lgan shifrlash uchun 44 ta kengaytirilgan kalitlar kerak bo'lar ekan. Raund kalitlari kengaytirilgan kalitlardan quyida bayon qilingan qoida asosida yaratiladi. Kalitlar generatsiyasining formulalari quyidagi ko'rinishlarga ega:

$$w[i]= w[i-1] \; ? \; w[i-N_k] ,$$

va

$$w[i]= SubWord (RotWord (w[i-1]))? Rcon[i/N_k]? w[i-N_k].$$

ISSN 2181-3187

Bizning holatda $N_k = 4$ bo'lganligi sababli i=4,8,12,16,20,… qiymatlar uchun formuladan foydalanib, kengaytirilgan kalitlar topiladi.
Ya'ni, i ning 4 ga karrali, 4 ga qoldiqsiz bo'linadigan qiymatlarida formuladan foydalaniladi. Qolgan barcha i=5,6,7,9,10,11,13,... qiymatlarida formuladan foydalaniladi. Bu yerda w(i) – 32 bit – so'zlardan iborat.
Masalan, biz ko'rayotgan holatda raund kalitining uzunligi 128 bit teng bo'lib, u to'rtta kengaytirilgan kalitga teng bo'ladi, ya'ni,
128 : 32 = 4 demak, w(i) = 1,2,3,4 w1=W1, W2, W3, W4, W5, W6, W7, W8, W9, W10, W11, W12, W13, W14, W15, W16, W17, W18, W19, W20, W21, W22, W23, W24, W25, W26, W27, W28, W29, W30, W31, W32;
w2=W33, W34, W35, W36, W37, W38, W39, W40, W41, W42, W43, W44, W45, W46, W47, W48, W49, W50, W51, W52, W53, W54, W55, W56, W57, W58, W59, W60, W61, W62, W63, W64;
w3=W65 , W66 , W67 , W68 , W69 , W7 , W71 , W72 , W73 , W74 , W75 , W76 , W77 , W78 , W79 , W80 , W81 , W82 , W83 , W84 , W85 , W86 , W87 , W88 , W89 , W9 , W91 , W92 , W93 , W94 , W95 , W96 ;
w4= W97 , W98 , W99 , W100 , W101 , W102 , W103 , W104 , W105 , W106 , W107 , W108 , W109 , W110 , W111 , W112 , W113 , W114 , W115 , W116 , W117 , W118 , W119 , W120 , W121 , W122 , W123 , W124 , W125 , W126 , W127 , W128 ;

0 – raund kaliti kirish kaliti	w0, w1, w2, w3.
1 – raund kaliti	w4, w5, w6, w7.
2 – raund kaliti	w8, w9, w10, w11.
3 – raund kaliti	w12, w13, w14, w15.
4 – raund kaliti	w16, w17, w18, w19.
5 – raund kaliti	w20, w21, w22, w23.
6 – raund kaliti	w24, w25, w26, w27.
7 – raund kaliti	w28, w29, w30, w31.
8 – raund kaliti	w32, w33, w34, w35.
9 – raund kaliti	w36, w37, w38, w39.
10 – raund kaliti	w40, w41, w42, w43.

1-jadval. Algoritm barcha raundi kalitlari

1-jadvalda raund kalitlari keltirilgan bo'lib, 0-raund kaliti boshlang'ich kirish kaliti hisoblanadi, to'q qora rang bilan berilgan kengaytirilgan kalitlar formuladan, qolgan kalitlar esa formuladan hisoblab topiladi.
formuladagi akslantirishlar quyidagi funktsiyalar asosida amalga oshiriladi:
- RotWord - 32 bitli so'zni bayt bo'yicha quyidagi ko'rinishda surish bajariladi {a0 a1 a2 a3}? {a1 a2 a3 a0};

ISSN 2181-3187

- SubWord ? S blokdan va SubBytes( ) funktsiyasidan foydalangan holda bayt bo'yicha akslantirish bajariladi.
- Rcon [j] = 2j-1, bu yerda j =(i / N_k) , i / N_k – bo'lish natijasi butun son chiqadi, chunki N_k =const bo'lib, i ning N_k ga karrali qiymatlari uchun bo'lish amali bajariladi.

Foydalanilgan adabiyotlar:

1. S. K. G'aniyev , M. M. Karimov, K. A. Tashev AXBOROT XAVFSIZLIGI << ALOQACHI>> -2008 71-73 b.
2. Kabulov A; Kalandarov I; Saymanov I; ,Models and algorithms for constructing the optimal technological route group equipment and the cycle of operation of technological modules,Smart transport conference 2022 Conference,,,1-11
3. Mirzoodilov, B.N.; Jo'raev M.T., Vasieva D.D. Saymanov IM ALGORITMICHESKAYA TEXNOLOGIYA ZASHITI INFORMATSIONNIX SISTEM NA BAZE TABLITSI FUNKTSIONIROVANIYA,AKTUAL`NIE VOPROSI SOVREMENNOY NAUKI I OBRAZOVANIYA,38,2020,