RC4 SHIFRLASH ALGORITMINING TAHLILI

Shukurov Dadanur Tohir o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti,
«Amaliy matematika va intellektual texnologiyalar» fakulteti 2-bosqich magistranti
E-mail: dadanur0094@gmail.com

ANNOTATSIYA

Buning uchun ishlab chiqilgan ko'plab kriptografik algoritmlar mavjud keng tarmoq orqali xavfsiz ma'lumotlarni uzatish. Ammo bu kriptografik algoritmlarning ba'zi kamchiliklari mavjud tajovuzkorlar tomonidan ma'lumotlarni olish uchun ishga tushirilgan. Shunday qilib bartaraf etish uchun kriptografik algoritmlarni kriptotahlil qilish kriptografik algoritmlarni qo'llashdan oldin yanada xavfsizroq bo'lishi mumkin. RC4 qanday ishlaydi va RC4 shifriga turli xil hujumlar. Biz ham RC4 uchun qo'llaniladigan turli kriptoanaliz usullarini o'rganamiz. RC4 da qo'llaniladigan texnikalar.

Kalit so'zlar: Kriptoanaliz, oqimli shifrlash, RC4.

RC4 dasturiy ta'minot tomonidan amalga oshirilgan birinchi oqim algoritmlaridan biridir. RC4 Lotus Notes, Apple Computer's AOCE, Oracle Secure SQL kabi o'nlab tijorat mahsulotlarida qo'llaniladi va CDPD uyali aloqa standart spetsifikatsiyasining bir qismidir.

RC4 algoritmini yaratish g'oyasi 1938 yilda R. A. Fisher va F. Yeyt tomonidan s<s[0]...s[m-l]> tasodifiy almashtirishni yaratish uchun tavsiflangan quyidagi konstruktsiyaga asoslangan . S_m, bu yerda s:j→s[j],j= 0,m-1.

Tasodifiy almashtirishni yaratish algoritmi uni (ASP deb ataymiz)

1.Dastlab s[0]=0, s[1]=1,..., s[m-1]=m-1 ni o'rnatamiz.

2.Uchun i=m -1, m- 2,...,1 bajaring:

a) $r_i \in Z_m$ tasodifiy sonni hosil qilish ;

b) $s[i] \Leftrightarrow s[r_i]$ transpozitsiyasini bajaring .

E'tibor bering, ba'zida 2-bosqich quyidagi transformatsiyani amalga oshiradi. i=m-1, m-2,...,1 uchun biz bajaramiz:

a) 0 va 1 orasida teng taqsimlangan Uj tasodifiy sonini hosil qilish ;

b) $r_i = [i*u_i]$;

c) $s[i] \Leftrightarrow s[r_i]$ transpozitsiyasini bajaramiz.

Yuqoridagilardan kelib chiqadiki, RC4 algoritmini o'rganish amaliy jihatdan muhim vazifa bo'lib, qo'shimcha ravishda uni tahlil qilish ham katta nazariy qiziqish uyg'otadi.

Quyidagi mualliflar tomonidan RC4 algoritmini tahlil qilish bo'yicha 1993-yildan 2003 yilgacha olingan asosiy natijalar keltirilgan: J. Golic, A. Shamir, S.Fluhrer, Knudsen L., Meier W., Preneel B., Rijmen V. , D McGrew, Verdoolaege S, I. Mantin va ularning dissertatsiya natijalari bilan aloqasi qayd etilgan.

RC4 tahlili natijalari keltirilgan.

-p ning boshlang'ich holatini yaratish algoritmining zaif tomonlarini tavsiflash va RC4 algoritmining kalitini topish usullarini ishlab chiqish;

-RC4 algoritmining dastlabki holatini tiklash usullarini ishlab chiqish ;

-RC4 gammasining statistik xususiyatlarini o'rganish . RC4 gammasini tasodifiy teng ehtimolli ketma-ketlikdan ajratish uchun statistik mezonlarni ishlab chiqish .

XULOSA

RC4 algoritmining dastlabki holatini yaratish usulining xususiyatlari tavsiflangan. Xususan, m uzunlikdagi RC4 algoritmining barcha kalitlari soni topiladi, bu o'zboshimchalik bilan belgilangan tsikl tuzilishi bilan dastlabki almashtirishlarga olib keladi. Olingan natijalar dastlabki almashtirishlarni taqsimlashda bir xil emasligini ko'rsatdi. Shunday qilib, bir xil boshlang'ich almashtirish eng katta ehtimolga ega ekanligi olinadi. Almashtirishdagi aniq nuqtalar qanchalik ko'p bo'lsa, uning paydo bo'lish ehtimoli shunchalik yuqori bo'ladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. A.A. Varfolomeev, A.E. Jukov, M.A. Pudovkin. Oqimli kriptotizimlar. Barqarorlik tahlilining asosiy xossalari va usullari - M: PAIMS-2000.

2. Golic, J. D, da'vo qilingan RC4 Keystream generatorining chiziqli statistik zaifligi.// Kriptologiyadagi yutuqlar - EUROCRYPT '97.

3. Fluhrer S., McGrew D. RC4 kalit oqimi generatorining statistik tahlili.// Kriptologiyadagi yutuqlar - FSE'2000- Springer-Verlag.

4. Knudsen L., Meier V., Preneel B., Rijmen V., Verdoolaege S, (da'vo qilingan) RC4 uchun tahlil usuli // ASIACRYPT'99-Springer-Verlag-1999.