ISSN: 3030-3346

BLOKLI SIMMETRIK SHIFRLASH ALGORITMLARINI KRIPTOTAHLIL QILISH MASALALARI

Xoliyorov Matyoqub Xurshid o‘g‘li

Qarshi davlat universiteti
E-mail: xoliyorovmatyoqub@gmail.com

K E Y W O R D S

blokli simmetrik shifrlash, kriptografiya, kriptotahlil, kriptobardoshlilik, shifrmatn, ochiq matn, maxfiy kalit, to‘liq tanlash usuli, chiziqli kriptotahlil, differensial kriptotahlil, algebraik kriptotahlil, hisoblash murakkabligi

A B S T R A C T

Ushbu maqolada blokli simmetrik shifrlash algoritmlarining kriptobardoshliligini baholashning zamonaviy usullari va ularning kriptotahlili tahlil qilingan. Kriptoanalitik ixtiyoridagi ma’lumotlar hajmi va turiga qarab shifrmatn, aniqlangan ochiq matn, tanlangan ochiq matn, tanlangan shifrmatn va tanlangan matn asosidagi hujumlarning o‘ziga xos xususiyatlari tavsiflangan. Shuningdek, to‘liq tanlov, statistik, chiziqli, differensial, chiziqli-differensial, slaydli, integral va algebraik kriptotahlil usullarining nazariy asoslari ko‘rib chiqilgan. Chiziqli va differensial kriptotahlil usullarining matematik mohiyati, ularni blokli shifrlash algoritmlarida qo‘llash imkoniyatlari hamda kalitni aniqlash jarayonidagi ahamiyati tahlil qilingan. Kriptografik algoritmning himoyalanganlik darajasini aniqlashda kalitlar fazosining hajmi, hisoblash murakkabligi, zarur bo‘lgan ochiq va shifrmatnlar soni hamda kriptotahlil uchun sarflanadigan hisoblash resurslari muhim mezonlar sifatida baholandi. Tadqiqot natijalari blokli simmetrik shifrlash algoritmlarini ishlab chiqish va ularning kriptobardoshliligini oshirish uchun kriptotahlil usullarini kompleks qo‘llash zarurligini ko‘rsatadi.

Kirish

Keyingi besh o‘n yilda kriptologiyaning barcha jabhalari bo‘yicha ilmiy izlanishlarning shiddat bilan o‘sishi bilan ajralib turadi. Kriptologiyaning kriptotahlil yo‘nalishi esa faol rivojlanayotgan tadqiqot sohasi bo‘lib qolmoqda. Axborot texnologiyalarining taraqqiyoti, hisoblash qurilmalarining takomillashuvi hamda kriptotahlil usullarining yutuqlari sababli, ilgari kriptobardoshli deb hisoblangan ko‘plab kriptotizimlar bugungi kunda ularga qo‘yilayotgan talablarga javob bera olmayapti.

1970-yillar boshigacha bo‘lgan davrda faqat simmetrik kalitli, ya'ni shifrlash va deshiflash uchun bitta kalit ishlatiladigan algoritmlariga asoslangan simmetrik kriptotizimlar ma'lum edi. Bundan tashqari axborotlar muhofazasi mavzusiga oid bo‘lgan ochiq ma'lumotlar juda kam ommalashtirilgan edi. Buning asosiy sababi, axborot texnologiyalari yutuqlarini ijtimoiy-iqtisodiy sohalarga keng qo‘llanilmaganligida, deb baholanadi.

1976-yilni kriptografiyada yangi davrning boshlanishi deb qarash mumkin. Chunki, shu yili U. Diffi va M.E. Xellmanning “Kriptografiyada yangi yo‘nalish” deb nomlangan maqolasining e'lon qilinishi ushbu sohadagi ochiq ilmiy ishlarning rivojini juda yuqori pog‘onaga ko‘tarilishiga olib keldi [3]. Ular o‘z ishlarida, maxfiy aloqa tizimlarida ma'lumotlarni shifrlash va deshifrlashda maxfiy kalitning tizim foydalanuvchilari orasida maxsus muhofazalangan aloqa kanali orqali uzatilishi va qabul qilinishiga hojat bo‘lmaydigan ilmiy-amaliy uslub asoslarini yaratib, bugungi kunda ham rivojlanib kelayotgan va dolzarb hisoblangan ochiq kalitli kriptografiya davrini boshlab berdi. Eslatib o‘tish joizki, R. K.Merklining U. Diffi va M.E.Xellmanga bog‘liq bo‘lmagan holda, lekin ular bilan deyarli bir paytda boshqa ilmiy jurnalga e'lon qilish uchun berilgan maqolasida ham ma'lumotlarni ochiq kalitli shifrlash g‘oyasining

(cc) BY

asoslari keltirilgan. Ammo R.K.Merkli maqolasining nashriyotda uzoq vaqt e'lon qilinmay to‘xtab qolishi, uni mualliflik huquqidan deyarli mahrum etdi [1-3].

Kriptotahlil yo‘nalishi kriptografiya yo‘nalishlariga mos ravishda turlicha bo‘lishi mumkin, ya'ni shifrlash algoritmi kalitini aniqlash, kriptografik algoritm yoki protokollarning nozik tomonlarini topish, shifrlangan ma'lumotlarni deshifrlash imkoniyatlarini yaratish va hakozo.

Kriptoalgoritmlar shifr matnlarga mos kelishi mumkin bo‘lgan tanlab olingan ochiq matnlar bilan kriptografik tahlil qilishga bardoshli bo‘lishi kerak. Bu talab, ma'lum algoritm bilan olingan bitta k kalit bilan biror shifrlab yuborilgan ma'lumotni k kalitni bilmagan holda uning ochilishiga erishilganda shu algoritm va shu kalit bilan shifrlab yuborilgan boshqa ma'lumotni ochilishiga olib bormasligi kerakligini bildiradi. Kriptotahlil usullari shifr matnni deshifrlash masalalarida biror algoritmning matematik modeli xususiyatlarini hisobga olgan holda qo‘llaniladi. Muvaffaqiyatli o‘tkazilgan kriptotahlil shifrmatn asosida ochiq matn va kalitni tiklash, shuningdek kriptoalgoritmning nozik joylarini topish imkonini beradi.

Kriptotahlil kriptoanalitik ega bo‘lgan ma'lumotlar asosida olib boriladi. Kriptoanalitik ega bo‘lgan ma'lumotlarga ko‘ra kriptotahlil turlari quyidagilardan iborat [5-7].

1. Kalit va shifrlash algoritmi haqida ma'lumotga ega bo‘lish maqsadida shifrmatnni tahlil qilish. Kriptoanalitikka faqat maxfiy kalitda shifrlangan shifrmatn ma'lum bo‘lib, shifrlash algoritmi ma'lum emas. Kalit va shifrlash algoritmi haqida ma'lumotga ega bo‘lish maqsadida kriptoanalitik shifrmatn parametrlarini ya'ni, shifrmatnning alfaviti yoki shifrbelgilarning shifrmatnda takrorlanishini sonli xarakteristikalarini (chastotalarini) aniqlab, ochiq matn qaysi tilda yozilganini, shifrlash turini, algoritmini va kalitini aniqlashga harakat qiladi.

2. Kalit haqida ma'lumotga ega bo‘lish maqsadida shifrmatnlarni tahlil qilish. Kriptoanalitikka bitta k maxfiy kalitda shifrlangan bir nechta shifrmatnlar $C_1,C_2,\ldots,C_i$ va shifrlash algoritmi ma'lum. Kriptoanalitikning vazifasi k-kalitni tiklashi kerak, ya'ni bitta k kalit va E akslantirish (shifrlash algoritmi) bilan $P_1, P_2, \ldots, P_i$ – ochiq matnlarga mos shifrmatnlar $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, $C_3 = E_k(P_3)$, …., $C_i = E_k(P_i)$ ma’lum bo‘lsa, noma’lum bo‘lgan ochiq matnlar: P_1 , P_2 ,...., P_i va k -kalitni topish zarur yoki $C_{i+1} = E_k(P_{i+1})$ tenglikdan P_{i+1} ni topish algoritmini yaratish kerak.

3. Kalit haqida ma’lumotga ega bo‘lish maqsadida ochiq matn asosida tahlil qilish. Kriptoanalitikka maxfiy kalitda shifrlangan bir nechta shifrmatnlar, shu shifrmatnlarga mos keluvchi ochiq matnlar hamda shifrlash algoritmi ma’lum.

Kriptoanalitikning vazifasi kalitni tiklashdan iborat. Demak, quyidagi ochiq matn va ularga mos keluvchi shifrmatnlar juftliklari: $(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3))$, $(P_i, C_i = E_k(P_i))$ hamda shifrlash algoritmi ma’lum bo‘lganda, noma’lum bo‘lgan k-kalitni yoki $C_{i+1} = E_k(P_{i+1})$ tenglikda noma’lum bo‘lgan P_{i+1} ochiq matnni topish imkonini beradigan algoritmni topish kerak.

4. Kalit haqida ma’lumotga ega bo‘lish maqsadida tanlab olingan ochiq matn asosida tahlil qilish. Kriptoanalitikka maxfiy kalitda shifrlangan shifrmatn, shifrlash algoritmi va kriptoanalitik o‘zi tanlab olgan ochiq matnlar, ya’ni: $(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3))$, $(P_i, C_i = E_k(P_i))$ kabi juftliklar ma’lum bo‘lib, kriptotahlil natijalariga qulaylik tug‘diruvchi xususiyatlarga ega bo‘lgan: P_1,P_2,P_3 ,...., P_i -ochiq matnlarni kriptoanalitikni o‘zi tanlab olish imkoniyati mavjud. Kriptoanalitikning vazifasi: yoki k-kalitni topish yoki $C_{i+1} = E_k(P_{i+1})$ tenglikdan P_{i+1} ni topish algoritmini yaratishdan iborat.

5. Kalit haqida ma’lumotga ega bo‘lish maqsadida tanlab olingan shifr matnlar asosida tahlil qilish. Kriptoanalitikka maxfiy kalitda shifrlangan bir nechta: $C_1, C_2,\ldots, C_i$ – shifr matnlar tanlab olib, ularning mos: $P_1 = D_k(C_1),\ldots, P_i = D_k(C_i)$ -ochik matnlarini xam olish imkoniyatiga ega. Kriptoanalitikning vazifasi k-kalitni topishdan iborat.

6. Kalit haqida ma’lumotga ega bo‘lish maqsadida tanlab olingan matnlar yordamida tahlil qilish. Kriptoanalitikka maxfiy kalitda shifrlangan shifrtekst, shifrlash algoritmi va 1) kriptoanalitik o‘zi tanlab olgan bir yoki bir necha ochiq va algoritm yordamida shifrlangan shifrmatn; 2) kriptoanalitik o‘zi tanlab olgan bir

(cc) BY

yoki bir necha shifrmatn va algoritm yordamida deshifrlangan ochiq matn ma’lum.

Demak $(P_1, C_1 = E_k(P_1))$,$(P_2, C_2 = E_k(P_2))$, $(P_i, C_{i1} = E_k(P_i))$ va $(C_1, P_1 = D_k(C_1))$, $(C_2, P_2 = D_k(C_2))$,...,$(C_i, P_i = D_k(C_i))$ juftliklar ma’lum. Kriptoanalitikning vazifasi k- kalitni topish.

7. Kalit haqida ma’lumotga ega bo‘lish maqsadida tanlab olingan kalitlar yordamida tahlil qilish.

Kriptoanalitikka maxfiy kalitda shifrlangan shifrmatn va shifrlash algoritmi ma’lum. Kriptoanalitik bir necha kalit tanlab oladi va algoritm yordamida maxfiy kalitga yaqin bo‘lgan kalitni topadi, ya’ni $(P_1, C_1 = E_{k1}(P))$, $(P_2, C_2 = E_{k2}(P))$, $(P_3, C_3 = E_{k3}(P))$,..., $(P_n, C_n = E_{kn}(P))$ ma’lum. k_1,k_2,k_3,…,k_n kalitlarning bog‘likliklari asosida shu shifrlash algoritmi bilan olingan ixtiyoriy C-shifrmatnni ochadigan k-kalitni yaratish algoritmini topish.

Bugungi kunda kriptotahlil usullarining ko‘plab turlari mavjud bo‘lib, ularning har biri kriptotahlilchining ixtiyoridagi ma’lumotlarga bog‘liq [3-5]. Kriptotahlilchining ixtiyoridagi ma’lumotlarning turi va hajmiga qarab, kriptotahlil usullarini bir necha guruhlarga bo‘lish mumkin. Ularning asosiy turlari 1-jadvalda keltirilgan.

1-jadval.

Kriptotahlil turlarining kriptoanalitik ixtiyoridagi ma’lumotlarga ko‘ra tasnifi

№	Kriptotahlil turi	Kriptoanalitikda mavjud ma’lumot	Asosiy maqsad
1	Faqat shifrmatn asosidagi tahlil	Shifrmatn	Algoritm va kalit xususiyatlarini aniqlash
2	Bir nechta shifrmatn asosidagi tahlil	Bir kalitda shifrlangan bir nechta shifrmatn	Maxfiy kalitni aniqlash
3	Ma’lum ochiq matn asosidagi tahlil	Ochiq matn va unga mos shifrmatn	Kalitni aniqlash
4	Tanlangan ochiq matn asosidagi tahlil	Kriptoanalitik tanlagan ochiq matn va mos shifrmatn	Kalitni aniqlash
5	Tanlangan shifrmatn asosidagi tahlil	Tanlangan shifrmatn va mos ochiq matn	Kalitni aniqlash
6	Tanlangan matn asosidagi tahlil	Tanlangan ochiq va shifrmatn juftliklari	Kalitni aniqlash
7	Tanlangan kalitlar asosidagi tahlil	Tanlangan kalitlar va shifrlash natijalari	Maxfiy kalit bilan bog‘liqlikni aniqlash

Shifrning u yoki bu tahlilga nisbatan kriptografik “chidamliligi” ning asosiy xarakteristikasi bu usulning $E(r)$ qiyinlilik darajasi bo‘ladi. Shifrlashni ochishning “qiyinlilik” darajasi o‘lchovi sifatida kalitni aniqlash yoki xabarni deshifrlash uchun zarur bo‘lgan elementar amallar soni qo‘llaniladi. Elementar amal deb aniq bir apparatura ishining bir qadamida bajariladigan operatsiyaga aytiladi. Shifrlash algoritmi shartsiz himoyalangan yoki absolyut mustahkam deyiladi, agar berilgan shifrlash algoritmi yordamida olingan shifrmatn mos ochiq matnni bir qiymatli tiklash uchun yetarli ma’lumotga ega bo‘lmasa, bunda shifrlangan matn hajmi hech qanday ahamiyatga ega emas. Bu shundan dalolat beradiki, kriptotahlilchi shifrni ochish uchun qancha vaqt sarflanmasin u shifrlangan matnni ochib tashlay olmaydi, chunki ochiq matnni tiklash uchun talab qilinadigan ma’lumot shifrmatnda yo‘q.

Foydalanuvchining u yoki bu shifrlash algoritmdan kutishi mumkin bo‘lgan himoyalanganlikning eng maksimum samaradorligi shundaki shifrlangan matnni ochish qiymati ochilgan ma’lumot qiymatidan oshib ketsa, shifrlangan matnni ochishga ketadigan vaqt ma’lumotning ishga yaroqlilik muddatidan oshib ketsa ikkita alomatidan hech bo‘lmasa birining bajarilishidir [7].

(cc) BY

Shifrlash algoritmlari himoyalangan deyiladi, agar u yuqorida ko‘rsatilgan talablarga mos kelsa. Muammo shundaki, aniq berilgan shifrlash algoritmi yordamida hosil qilingan shifrmatn kriptotahlil uchun kerak bo‘lgan harakatlarni sonli baholash juda qiyin [7].

Kriptotahlilning deyarli barcha turlari blokli shifrlash algoritmlari uchun ochiq matn tuzulishining o‘ziga xosliklari shifrlashda saqlanib qolishi va hosil qilingan shifrmatn tuzulishi o‘ziga xosliklarda paydo bo‘ladi.

To‘liq tanlash (perebor) usuli. Kriptotahlilchining shifrlash algoritmini bilgan holda shifrmatnni barcha mumkin bo‘lgan kalitlar bilan deshifrlashiga asoslanadi. Misol uchun kalit uzunligi 100 bit bo‘lsa, barcha kalitlar soni 2^{100} ga teng, ya’ni kalitlar to‘plami quvvati|K|=2^{100} ga teng bo’ladi [2,3,5].

Chiziqli kriptotahlil usuli. 1990-yilda yaponiyalik kriptograf M.Matsui tomonidan taklif etilgan bo‘lib, bu usulda kriptotahlilchiga shifrmatn, kriptotahlilchi tomonidan tanlab olingan ochiq matn va algoritm ma’lum bo‘lishi kerak. Kriptotahlilchining vazifasi

$$X[i_1, i_2,\dots, i_n] \oplus Y[j_1, j_2,\dots, j_m] = K[k_1, k_2,\dots, k_l] \quad (1)$$

$$X[i_1, i_2,\dots, i_n] = X[i_1] \oplus X[i_2] \oplus \dots \oplus X[i_n]$$
$$Y[j_1, j_2,\dots, j_m] = Y[j_1] \oplus Y[j_2] \oplus \dots \oplus Y[j_m]$$
$$K[k_1, k_2,\dots, k_l] = K[k_1] \oplus K[k_2] \oplus \dots \oplus K[k_l]$$

tenglikdan eng yaqin chiziqli approksimatsiyani, ya’ni tahlil qilinayotgan algoritm akslantirishlarining xossalaridan kelib chiqib, eng samarali natija beruvchi chiziqli bog‘lanishni tanlab olishdir [2-6].

Differensial kriptotahlil usuli. E.Biham va A.Shamir tomonidan taklif etilgan bo‘lib, bu usulni amalga oshirish uchun shifrmatn, ochiq matn(tanlab olingan) va algoritm kerak bo‘ladi. Differensial kriptahlil usuli raundga asoslangan bloklab shifrlash algoritmlari bilan shifrlanadigan shifrmatnlarni ochishga qo‘llanilgan. Bu usulda ikkita ochiq matn X, X^1 va biror kalit bilan shifrlangan $Y = F(X, K), Y^1 = F(X^1, K)$ shifrmatnlar orasida ayirma amali aniqlanadi

$$\begin{cases} \Delta X = X \oplus X^1 \\ \Delta Y = Y \oplus Y^1 \end{cases} \quad (2)$$

va ΔX,ΔY qiymatlar orasidagi moslik orqali kalit tiklanadi. Agar algoritm bir necha raunddan iborat bo‘lsa, hisoblashlar har bir raundga qo‘llaniladi. Har bir raund uchun X(i), X^1(i) ochiq matn, Y(i), Y^1(i) shifrmatn va Y(i), Y^1(i) matnlar $i+1$ −raund uchun ochiq matn hisoblanadi $Y(i) = X(i+1)$, $Y^1(i) = X^1(i+1)$. Ayirma har bir raund uchun quyidagicha hisoblanadi

$$\begin{cases} \Delta X(i) = X(i) - X(i)^1 \\ \Delta Y(i) = Y(i) - Y(i)^1 \end{cases} \quad (3)$$

Bu usul birinchi marta DES kriptoalgoritmiga Ye.Biham, A.Shamir tomonidan qo‘llanilgan[2-6].

Foydalanilgan adabiyotlar

1. Akbarov D.Ye. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent, “O‘zbekiston markasi” nashriyoti, 2009. 432bet.
2. Алферов А.П. и др. Основы криптографии: Учебное пособие. М., Гелиос АРВ, 2002. 480с.
3. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М., «Гелиос АРВ», 2006. 376 с.
4. Boymirzayev N. Ayirma matritsa va ularning simmetrik shifrlash algoritmlari kriptobardoshligini baholashdagi qo‘llanishlari. Axborot xavfsizligi yo‘nalishi bo‘yicha magistr darajasidagi dissertatsiya ishi. Toshkent, 2010 y. 115 b.
5. Kuryazov D.M. “Amaliy Kripto tahlil” SD-07 fanidan ma’ruzalar to‘plami. Toshkent, ATM, 2011y. 98 bet.
6. Sattarov A.B. “Blokli simmetrik shifrlash algoritmlari uchun chiziqli differensial kriptotahlil usulini qo‘llash va uning dasturiy ta’minotini yaratish”. Axborot xavfsizligi yo‘nalishi bo‘yicha magistr darajasidagi dissertatsiya ishi. Toshkent– 2011. 100 bet.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М., Изд. ТРИУМФ, 2003. 816 с.

(cc) BY