“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 1, 2024. JANUARY
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

KRIPTOGRAFIK ALGORITMLAR

TerDU, Kompyuter tizimlari va ularning dasturiy ta’minoti yo‘nalishi magistranti Boboyeva Fotimaxon Abdumurot qizi
TerDU, Kompyuter tizimlari va ularning dasturiy ta’minoti yo‘nalishi magistranti Allanazarova Davlatoy Farxod qizi

Annotatsiya: Qadim zamonlardan beri inson mo‘jizalar, sirli voqea va hodisalar sababi hamda mohiyati haqida axborot olishga intilgan. Axborot inson tili va yozuvida o‘z aksini topadi. Dastlabki yozuvlar o‘ziga xos bo‘lgan kriptografik tizim bo‘lib, qadimgi jamoalarda ularni faqat nufuzli shaxslargina tushunishgan. Qadimiy Misr va Hindistonda mavjud bo‘lgan ilohiy kitoblar bunga misol bo‘la oladi. Ushbu maqolada Kriptografik algoritmlar haqida ma’lumot berilgan.

Kalit so‘zlar: Kriptografik algoritmlar, kriftografika, xabar, Kriptografiya tarixi, Dastlabki kriptografiya, Formal kriptografiya, Ilmiy kriptografiya

Bundan 4000 yil avvalgi davrga oid eng qadimiy shifrmatn Messopatamiya qazilmalarida topilgan. Unda loydan ishlangan taxtachada o‘ymakor yozuvda tijorat siri – kulolchilik buyumlarini glazurlash resepti yozilgan. Qadimiy Misrda shifrlangan diniy matnlar va tibbiy reseptlar ham mavjud bo‘lgan. Kriptologiya (grekchada kryptos - “sirli” va logos -“xabar”) deganda aloqa xavfsizligi haqidagi fan tushuniladi. U aloqa kanallari orqali axborotning xavfsizligini ta’minlab saqlash hamda uzatish tizimlarini yaratish va tahlillash to‘g‘risidagi fandir. Kriptologiya ikki ilmiy irmoqqa ajraladi. Bular kriptografiya va kriptotahlildir [1-10]. Kriptografiya axborot almashtirish tamoyillari, vosita va usullari bilan shug‘ullanadigan fan sohasi bo‘lib, uning maqsadi axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash va axborotni buzishning oldini olish hisoblanadi. Kriptotahlil shifrni yoki har qanday boshqa shakldagi kriptografiya obyektining sirini ochish san’ati va ilmi bo‘lib, kalitni bilmasdan turib shifrlangan matndan dastlabki matnni olish yoki dastlabki matn va shifrlangan matn bo‘yicha kalitni hisoblash jarayonidir. Kriptotahlil usullari tarixi kriptografiya tarixi bilan egizdir. Kalitdan foydalangan holda alohida qoidalar bo‘yicha ochiq (dastlabki) ma’lumotlar to‘plamini shifrlangan ma’lumotlar to‘plamiga almashtirish uchun amalga oshiriladigan qaytar

almashtirishlar majmui shifr deb ataladi. Dastlabki ochiq matnni uning ma’nosini berkitish maqsadida shifrlangan ma’lumotga o‘girish natijasi shifrmatn (shifrma’lumot) deb ataladi. Keng ma’noda axborotni shifrlash deganda shifrmatnga o‘girish jarayoni tushuniladi.

Kriptografiya tarixi. Ming yilliklar davomida kriptografiyadan davlat qurilishida, harbiy va diplomatiya aloqasini muhofazalashda foydalanib kelingan bo‘lsa, axborot asrining boshlanishi bilan kriptologiya jamiyatda, xususiy sektorda foydalanish uchun ham zarur bo‘lib qoldi [14-15]. Qariyb 35 yildan buyon kriptologiyada keng miqyosda ochiq tadqiqotlar olib borilmoqda. Hozirgi kunda konfidensial axborot (masalan, yuridik hujjatlar, moliyaviy, kredit stavkalari to‘g‘risidagi axborotlar, kasallik tarixi va shunga o‘xshash)larning talay qismi kompyuterlararo odatdagi aloqa kanallari orqali uzatilmoqda. Jamiyat uchun bunday axborotning konfidensialligi va asl holda saqlanishi zaruratga aylangan. Kriptografiya tarixini shartli ravishda 4 bosqichga bo‘lish mumkin [1, 3-6]:

1. Dastlabki kriptografiya.
2. Formal kriptografiya.
3. Ilmiy kriptografiya.
4. Kompyuter kriptografiyasi, bu bosqich kriptografiyada simmetrik va nosimmetrik kriptotizimlar bo‘yicha ikki ilmiy yo‘nalish yuzaga kelishi bilan xarakterlanadi.

Kriptoalgoritmlar, xususan, blokli simmetrik shifrlash algoritmlari DES, AES, GOST 28147-89, O‘z DSt 1106:2009, mos ravishda 56 bit, 128, 256 bit yoki 512 bit, 256 bit, 256 yoki 512 bit uzunlikdagi oldindan belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan kalitlardan foydalanadi. Biroq standart algoritmlarda belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan barcha kalitlar har doim ham shifrmatnni ochish maqsadida ochiq aloqa tarmog‘ini nazorat qiluvchi kriptotahlilchi tomonidan uyushtiriladigan turli kriptohujumlarga bardoshli bo‘lmasligi mumkin. Masalan, kalitni tashkil etuvchi bitlar ketma-ketligi faqat nollardan yoki birlardan yoki bo‘lmasa, nol va birlarning kombinasiyasi fiksirlangan davr bilan takrorlanishi yordamida tuzilgan bo‘lsa, bu toifa kalitlar bardoshsiz hisoblanadi. Chunki ushbu tur bitlar ketma-ketligida, shu ketmaketlikni tashkil etuvchi nol va bir elementlari davriy takrorlanishining matematik qonuniyatini oldindan bilish imkoniyati mavjud. U holda bu zaylda generasiya qilingan bitlar

ketma-ketligidan simmetrik shifrlash algoritmlari uchun maxfiy kalit sifatida foydalanish maqsadga muvofiq emas.

Grafik testlar - Grafik testlar foydalanuvchiga tekshirilayotgan ketmaketlikning ma'lum bir grafik bog'liqligi haqidagi ma'lumotni berib, u bo'yicha tekshirilayotgan ketma-ketlik xossalari to'g'risida xulosa chiqarish imkoniyatini beradi.

Baholash testlari - Baholash testlari tekshirilayotgan ketma-ketlik statistik xossalarini tahlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi [12-13].

Quyida misol sifatida bir tomonlama funksiyalarga asoslangan psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar keltirib o'tiladi [13]:

1) ANSI X9.17 generatori. Bu algoritm AQShda psevdotasodifiy ketmaketlik ishlab chiquvchi Milliy standart hisoblanib, FIPS (USA Federal Information Processing Standart) tarkibiga kiradi. Algoritmda bir tomonlama funksiya sifatida 3DES ikkita K1, K2∈V64 kalit ishlatiladi: DESK1DESK2 DESK1(64 bit) .

2) FIPS-186 generatori. Bu algoritm ham AQSh Milliy standarti sifatida qabul qilingan bo'lib, DSA elektron raqamli imzo algoritmining maxfiy parametrlarini va kalitlarini generasiya qilish uchun mo'jallangan. Algoritm bir tomonlama funksiya sifatida DES shifrlash algoritmi va SHA-1 xeshlash algoritmini ishlatadi. 3) Yarrow-160 generatori. Yarrow-160 psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatori Kelsi, Shnayer va Fergyuson tomonidan taklif qilingan. Bu yerda uchlik DES va SHA-1 xeshlash algoritmi ishlatilgan. Sonlar nazariyasi muammolariga asoslangan generatorlar sifatida:

1) **RSA algoritmi asosidagi**;

2) **Mikali-Shnorr RSA algoritmi** asosidagi;

3) **BBS (Blum-Blum-Shub)** - algoritmi asosidagi generatorlarni keltirish mumkin.

Xulosa qilib shuni aytish mumkinki, Ming yilliklar davomida kriptografiyadan davlat qurilishida, harbiy va diplomatiya aloqasini muhofazalashda foydalanib kelingan bo'lsa, axborot asrining boshlanishi bilan kriptologiya jamiyatda, xususiy sektorda foydalanish uchun ham zarur bo'lib qoldi. Qariyb 35 yildan buyon kriptologiyada keng miqyosda ochiq tadqiqotlar olib borilmoqda. Hozirgi kunda konfidensial axborot (masalan, yuridik hujjatlar, moliyaviy, kredit stavkalari

to‘g‘risidagi axborotlar, kasallik tarixi va shunga o‘xshash)larning talay qismi kompyuterlararo odatdagi aloqa kanallari orqali uzatilmoqda. Jamiyat uchun bunday axborotning konfidensialligi va asl holda saqlanishi zaruratga aylangan. Kriptografiya tarixida birinchi muhim voqyea simmetrik kriptotizimlarning birinchi marta Davlat standarti maqomiga ega bo‘lishi bo‘lsa, keyingi o‘n yilliklarning muhim kashfiyoti kriptologiyaga yangicha yondashuvlarni boshlab bergan oshkora kriptografiyaning yuzaga kelib uning muttasil rivojlanib borayotganligidir. AQShdan keyin Yevropa davlatlari va Yaponiyada elektron raqamli imzo bo‘yicha qonun va dastlabki davlat standartlari qabul etildi. Ko‘pchilik davlatlar, shu jumladan O‘zbekiston Respublikasi ham kriptografiya vositalaridan axborot–telekommunikasiya tarmoqlarida maxfiy axborotlarni xavfsiz uzatish va elektron raqamli imzo yaratishda o‘z milliy algoritmlaridan foydalanmoqdalar.

FOYDALANILGAN ADABIYOTLAR

1. Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4947-сон фармони. Тошкент, 2017 йил 7 феврал.

2. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Дастлабки ва формал криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №1 (4). – 32-37 -бетлар.

3. Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.

4. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – Москва: Лори Гелиос АРВ, 2002. – 240 с.

5. Бабаш А.В., Шанкин Г.П., Криптография – Москва: Лори Гелиос АРВ, 2002. – 512 с.

6. Арипов М.М., Пудовченко Ю.Е. Основы криптологии – Ташкент: 2004. – 136 с.

7. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.

8. Алексеев А. Криптогрфия и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html

9. Жельников В. Криптогоафия от папируса до компьютера. М.:ABF, 1996.

10. O‘z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар».

11. История криптографии и криптоанализа. http://crypto hot box.ru.

12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

13. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

14. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

15. «Ошкора калитли криптотизимларни криптотаҳлиллаш учун қуролу-воситалар ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-8 -босқич ҳисоботлари. – ЎзААА ФТМТМ, Тошкент, 2003.

16.Защита информации. Малый тематический выпуск. ТИИЭР, 1988 г, т.76, №5.

17.Kahn D. The codebreakers. N.-Y., 1967.

18. Саломаа А. Криптография с открытым ключом. М.,1997

19. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. О развитии криптографии в XIX веке. Защита информации. Конфидент. 2003 г. №5.

20. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. Криптографические идеи XIX века. Защита информации. Конфидент. 2004 г. №1, №2.

21. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Илмий криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №2 (5). – 47-53 бетлар.

22. Михаил Масленников. Практическая криптография. СанктПетербург «БХВ-Петербург», 2003.

23. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – 59-74 бетлар.