Xulosa. Keltirib o‘tilgan algoritmlardan foydalanib tasvirlarni filtrlash orqali tanib olish amalga oshirilganda yahshi natijalarga erishildi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Шлихт Г.Ю. Цифровая обработка цветных изображений. - М., Издателство ЕКОМ, 1997. - 336 с. 2. Яне, Б. Цифровая обработка изображений / Б. Яне: пер. с англ. под ред. А.М.

2. Измайловой. М.: Техносфера, 2007 - 584с.-ИСБН 978-5-94836122-2

3. Кравченко В.Ф. Цифровая обработка сигналов и изображений. - М.: ФИЗМАТЛИТ, 2007 г.

4. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). Image contour separation algorithms based on the theory of fuzzy sets. International Journal of Contemporary Scientific and Technical Research, 120-125.

5. Axbutayevich, T.S., & Abdumalikovich, Q.N. (2022). Tasvirlardan ma’lumot olishda matlab muhitining intellektual tashkil etuvchilaridan foydalanish. International Journal of Contemporary Scientific and Technical Research, 247- 250.

6. Akhbutayevich, T. S., & Abdumalikovich, K. N. (2022). Algorithms for Selecting the Contour Lines of Images Based on the Theory of Fuzzy Sets. Texas Journal of Engineering and Technology, 15, 31-40.

NOSIMMETRIK SHIFRLASH ALGORITMLARI ASOSIDA YOTUVCHI ALGEBRAIK STRUKTURALARNING TAHLILI

t.f.n., dots. Tavboyev Sirojiddin Axbutaevich,
Eshonqulov Sherzod Ummatovich,
Qarshiboyev Nizomiddin Abdumalik o‘g‘li
Jizzax politexnika instituti
wolkswagen1991@mail.ru

Annotatsiya: Maxfiylik foydalanuvchi, masalan, elektron raqamli imzo (ERI) sohibining shaxsiy maxfiyligi bo‘lib, uning oshkora kalitini ERI shakllantirishda bevosita foydalaniladi.

Kalit so‘zlar: Shifr, kriptografiya, kriptoanaliz, funksiya, ERI haqiqiyligi, kalit, algoritmlar.

Nosimmetrik kriptotizimlarning matematik asosi bo‘lib chekli maydon, gruppa, qismgruppa ko‘rinishidagi algebraik strukturalar va ularda kriptografik algoritmga asos qilib olingan modul arifmetikasining maxfiylik (sekret, lazeyka)ka ega bir tomonlama funksiya xizmat qiladi.

Bir tomonlama funksiya - shunday $y = f(x)$ funksiyaki, uning aniqlanish sohasidan bo‘lgan ixtiyoriy x uchun $f(x) = y$ qiymat oson hisoblanadi, qiymatlar sohasining barcha y qiymatlariga mos keluvchi x qiymatlarni hisoblash esa amaliy jihatdan murakkab bo‘lgan masala (muammo)ni echishni talab etadi.

Ushbu algebraik strukturalarni hisoblash murakkabligi orqali ochiq kalitli kriptotizimlarga asoslangan algoritmlarning ishonchlilik, bardoshlilik darajasi o‘lchanadi.

Shaxsiy maxfiylikning shaxsga bog’liqligi axborot xavfsizligini ta’minlashning zaruriy shartidir. Oshkora kalit ERI haqiqiyligini tasdiqlash (verifikatsiyalash), ma’lumot manbaini autentifikatsiyalash, maxfiy kalitlarni almashish va boshqa vazifalarni hal etish uchun nosimmetrik kriptografiyaning asosiy tizimli parametridir.

Bir tomonlama funksiyalarning birinchi turi $y \equiv a^x (mod\ p)$ tub maydon $F(p)$ hosil qiluvchi element a ni maxfiy x darajaga oshirish funksiyasi ko‘rinishida U. Diffi va M. Xellman tomonidan taklif etilgan, bu erda (a, y, p) oshkora parametrdir. Ular sub’ektlar jufti A va B orasida umumiy kalit o‘rnatish masalasini har bir sub’ekt tomonidan mos tarzda, $y_A \equiv a^{xA} (mod\ p)$ va $y_B \equiv a^{xB} (mod\ p)$ funksiyalarni hisoblashga, so‘ngra ularni oshkora kanal orqali ayirboshlashga va sub’ektlar juftligining har biri tomonidan umumiy maxfiy kalitni, mos tarzda, $K_A \equiv y_B^{xA} (mod\ p)$, $K_B \equiv y_A^{xB} (mod\ p)$ ifodalar bo‘yicha hisoblashga keltirishgan, bu erda $K_A q\ K_B$.

U. Diffi va M. Xellman o‘zlari nomida ta’riflangan diskret logarifm muammosiga teng kuchli muammoni ham ilgari surdilar:

agar tub modul p, $GF(p)$ chekli maydonning hosil qiluvchi (generator) elementi a va diskret darajaga oshirish funksiyalari qiymatlari $y_A \equiv a^{xA} (mod\ p)$ va $y_B \equiv a^{xB} (mod\ p)$ berilgan bo‘lsa, unda $y_A \equiv a^{xA} (mod\ p)$ va $y_B \equiv a^{xB} (mod\ p)$ topilsin.

Keyinroq, U. Diffi va M. Xellmanning bir tomonlama funksiyasi asosida turk millatiga mansub Toxir Al Jamol tomonidan kriptografiya tarixida birinchi ERI - EGSA yaratildi. Mazkur algoritm shifrlash maqsadlarida ham foydalanish imkoniyatiga ega bo‘lib, u ba’zi o‘zgartirishlar bilan AQSh davlat standarti DSA va Rossiya Federatsiyasi standarti GOST 34.10-94 ga asos qilib olindi. Kiritilgan o‘zgartirishlardan birinchisi malumotning xesh-qiymatidan foydalanish bo‘lsa, ikkinchisi ERI ikkinchi komponentasi uzunligini qisqartirish maqsadida K. Shnorr g’oyasidan, ya’ni $p-1$ o‘rniga uning eng katta tub faktoridan foydalanishdir.

Bu algoritmlarning bardoshliligi foydalanilgan xesh-funksiyaning bardoshliligi va diskret logarifmlash muammosining hisoblash murakkabligi, ya’ni $x \equiv log_a y (mod\ p)$ ni hisoblash murakkabligi bilan belgilanadi. Hozircha $p > 2^{530}$ uchun effektiv hisoblash algoritmi ishlab chiqilmagan.

Nemis olimlari 530 bitli (160 o‘nli xonali) tub modul p uchun diskret logarifmlash muamosini hal etishgani haqida ma’lum etilgan. Bu esa diskret logarifm muammosiga asoslangan algoritmlarning kriptografik bardoshliligi va xavfsizlik parametrlariga bo‘lgan talablarni kuchaytirishga olib keladi.

1973 yilda Britaniya davlat GCHQ agentligining kriptologi Klifford Koks aslida oshkora kriptotizimni bayon etuvchi yopiq hujjatni tayyorladi [1]. Bu kriptotizim bardoshliligi K. Koks tomonidan taklif etilgan bir tomonlama funksiyaning ikkinchi turiga, ya’ni faktorlash muammosining murakkabligiga asoslangan.

1977 yilda amerikalik R. Rayvest, A. Shamir, L. Adleman tomonidan bir tomonlama funksiyalarning ikkinchi turi $yqf(d) (mod\ n)$ ko‘rinishda taklif etilgan va ular tomonidan shifrlash va ERI algoritmi RSA ishlab chiqilgan. RSA algoritmida modul $nqpq$ bo‘lib, bu erda p, q har xil tub sonlardir. Lekin, K. Koks tomonidan avvalroq RSA algoritmiga o‘xshash algoritm yaratilganligi RSA mualliflarining

shuhratiga soya sola olmaydi, chunki ular maxfiy ishlanmani bilmagan holda o‘z algoritmlarini mustaqil yaratganlar. Algoritmda oshkora kalit sifatida *(n, e)* juftlikdan, shaxsiy kalit sifatida (*d, φ(n))* juftligidan foydalaniladi, bu erda *(d, e)* - bir-biriga modul *φ(n)* bo‘yicha multiplikativ teskari butun sonlar jufti, *φ(n) q (p-1)*(q-1)* - Eyler pi-funksiyasi.

Algoritmning asosiy protseduralari xeshlash va modul arifmetikasida butun sonli halqada darajaga oshirishdan iborat.

RSA algoritmi qisqa ma’lumotlarni shifrlash uchun ham foydalaniladi. Bu holda ma’lumot *M* ni uzatuvchi tomon shifrmatn $Sh \equiv M^e \pmod n$ ifoda bo‘yicha hisoblasa, shifrmatn qabul qiluvchi tomon, ya’ni oshkora va shaxsiy kalit egasi $M \equiv Sh^d \pmod n$ ifoda asosida *M* ni tiklaydi.

RSA algoritmining bardoshliligi foydalanilgan xesh-funksiyaning bardoshliligi va faktorlash muammosining hisoblash murakkabligi, ya’ni *n* bo‘yicha *p* va *q* ni topish murakkabligi bilan belgilanadi. Hozircha $n>2^{1024}$ uchun effektiv kriptotahlil algoritmi ishlab chiqilmagan.

RSA algoritmining kamchiliklariga *n* va *d* generatsiyalash bosqichida ko‘pgina hali ham o‘sishda davom etayotgan qo‘shimcha shartlarni tekshirish zarurligi bo‘lsa, afzalligi - verifikatsiya jarayoniga juda kam vaqt sarflanishidir, chunki ko‘pincha *eq3* yoki $2^{16}Q1$ ko‘rinishida tanlanadi.

Nosimmetrik kriptografiya yuzaga kelgandan buyon o‘tgan davr ichida ERI algoritmlarining juda ko‘p rusumlari taklif qilingan. Ular bir-biridan, asosan, bir tomonlama funksiya turi va har xil hujumlarga nisbatan bardoshlilikni ta’minlovchi muammo turi bilan farqlanadi. Bu davrga tegishli ERI algoritmlarining asosiy ko‘pchiligini uch sinfga ajratish mumkin: diskret logarifmlash muammosining murakkabligiga asoslangan sxemalar; faktorlash muammosining murakkabligiga asoslangan sxemalar; diskret logarifmlash va faktorlash muammolarining kompozitsiyasi murakkabligiga asoslangan sxemalar.

Diskret logarifmlash muammosining murakkabligiga asoslangan sxemalar ERI EGSA sxemasi asosida shakllangan umumiy sxemaning 120 rusumdan iborat xususiy hollaridir.

RSA sxemasidan keyin yuzaga kelgan faktorlash muammosining murakkabligiga asoslangan sxemalar, masalan, ESIGN kabi sxemalar, o‘z mohiyati bo‘yicha RSA sxemasining ba’zi modifikatsiyalaridir.

Diskret logarifmlash va faktorlash muammolarining kompozitsiyasi murakkabligiga asoslangan sxemalar ham e’tiborga loyiq. Ularning farqli tomoni shundaki, ERIning ikkala tashkil etuvchisi *(r, s)* EGSAdan farqli o‘laroq, bir vaqtda shakllantiriladi. Bunday ERI sxemasining ahamiyatli tomoni shundaki, muammolar kompozitsiyasini tashkil etuvchi biror muammoni effektiv hal etish kriptotizimning to‘la barbod bo‘lishiga olib kelmaydi, bardoshlilik qolgan muammo murakkabligigacha pasayadi.

Elliptik egri chiziq nazariyasini yaratishda so‘nggi ulug’ qadimiy grek matematigi Diofantdan boshlab o‘tmishning ko‘pgina eng yirik olimlari qatnashgan. O‘tgan asrning 80 yillarida EECh katta sonlarni faktorlash algoritmlarini tuzish sohasida qo‘llanila boshladi va bu qo‘llanishlar orqali kriptografiya sohasiga kirib keldi (nosimmetrik tizimlar, psevdotasodifiy sonlarni generatsiyalash). Elliptik

kriptografiyada haqiqiy burilish 1985 yilda N. Koblits va V. Miller ilmiy ishlari [2] chop etilgandan so‘ng yuz berdi. Shu damdan boshlab mashhur jahon kriptologlari elliptik kriptografiya bilan shug’ullana boshladilar.

Faktorlash va EECh gruppasida diskret logarifmlash murakkabliklarini taqqoslama tahlili EEChlarning bahslashuvdan holi afzalliklarini namoyon etdi [3,4]. 1-jadvalda taqqoslama ma’lumotlar keltirilgan (ma’lumotlar tub maydonda diskret logarifmlash muammosi uchun ham oson hisoblanadi).

1-jadval

Kriptotahlil murakkabliklari bo‘yicha ma’lumotlar

Almashtirish moduli uzunligi	EECh gruppasida kriptotahlil murakkabligi	RSA modulini faktorlash murakkabligi
192 bit	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 bit	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 bit	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 bit	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

XXI asrning boshidan boshlab nosimmetrik kriptografiyaning an’anaga aylanib qolgan kriptotizimlardan bardoshliligi EECh gruppasida diskret logarifmlash muammosining murakkkabligiga asoslangan tizimlarga o‘tish boshlangani ko‘zga tashlandi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. “O‘zbekiston markasi “, 2009. - 432 b.

2. O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari».

3. Брюс Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ - Москва: ТРИУМФ, 2002.

4. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. - Toshkent, 2008. 208 b.

ENSURING A SAFER DIGITAL FUTURE, THE IMPORTANCE OF CYBERSECURITY EDUCATION

(PhD) Mukhtarov Farrukh Mukhammadovich
The Ferghana Branch Tashkent university of information technologies
fmm1980@rambler.ru

Annotation: This article discusses the importance of cybersecurity education in today's digital world. It defines cybersecurity education and explains its benefits, such as reducing the risk of cyber attacks, protecting sensitive data, and minimizing the damage caused by a cyber attack. The article also provides a list of common cyber threats, such as phishing attacks, malware, and ransomware.