AXBOROT XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY USULLARI VA TEXNOLOGIYALARI

Suyunov Akmal Xo’shboq o’g’li
TerDU 1-bosqich magistranti
suyunovakmal27@gmail.com

Annotatsiya: *Maqolada axborot xavfsizligini ta’minlashda qo‘llaniladigan usul va texnologiyalar keng qamrovli bayon etilgan. Shuningdek, axborot tizimlarida, kiber xavfsizlikni ta'minlash uchun ma’lumotlarni turli algoritmlar yordamida shifrlash usullari batafsil yoritilgan.*

Kalit so’zlar. *Axborot, axborot xavfsizligi, kriptografiya, autentifikatsiya, parollar, shifirlar, kalit so'zlar, asimmetrik shifrlash va simmetrik shifrlash.*

Kirish. Hozirgi globallashuv davrida, har qanday taraqqiy etgan jamiyat hayotida axborotning ahamiyati uzluksiz ortib bormoqda. Axborot xavfsizligini ta'minlashning zamonaviy usullari va texnologiyalari turli soha va tarmoqlarda keng qo‘llanilmoqda. Bu texnologiyalar ma'lumotlarni himoyalash, maxfiylikni ta'minlash, tizimlarga ruxsatsiz kirishni oldini olish, hamda biznes va davlat sektorlarida xavfsiz operatsiyalarni amalga oshirishga yordam beradi. Shuningdek, hozirgi vaqtda axborot texnologiyalarini avtomatlashtirish va axborotni muhofaza qilish yo’nalishlari muntazam mukammallashib bormoqda.

Adabiyotlar sharhi. Axborot xavfsizligi sohasida yirik olimlar va ularning ishlari bugungi kunda global xavfsizlik tizimlarining asosi hisoblanadi. Uitfild Diffi va Martin Hellmanning Diffi-Xellman(1976) algoritmi, kriptografiya tizimlarida ochiq kalit almashish imkonini beribgina qolmasdan shifrlash xavfsizligini oshirdi, hamda algoritm simmetrik kalitlarni xavfsiz tarzda almashish imkoniyatini yaratdi. Biroq, bu algoritm man-in-the-middle (aralashuvchi shaxs) dan keladigan tahdidlarga bardoshsiz bo'lib, uni yanada xavfsiz qilish uchun qo'shimcha autentifikatsiya usullarini talab qiladi. Ron Rivest, Adi Shamir va Leonard Adleman (RSA) 1978 yilda dunyodagi eng

mashhur va keng qo'llaniladigan asimmetrik kriptografik tizimini yaratdilar. RSA algoritmi ochiq kalitli shifrlashning eng keng qo`llaniladigan usullaridan biri bo'lib, xavfsiz aloqani ta`minlaydi, qolaversa RSA algoritmi ko'plab xavfsizlik standartlarida foydalaniladi va juda ishonchli hisoblanadi. Kamchiliklari, algoritmning tezligi past bo‘lib, katta hajmdagi ma’lumotlar uchun samaradorligi kamayadi va kvant kompyuterlar rivojlanishi bilan RSA ning xavfsizligi zaiflashishi mumkin. Ralf Merkle (Merkle daraxtlari) ning axborot tizimlari himoyasidagi blokcheyn texnologiyasi, ma’lumotlarni markazlashmagan tarmoqda saqlab, soxtalashtirish va o‘zgartirishni juda murakkab holga keltiradi. Ayniqsa, moliyaviy va tijorat sohalarida tranzaksiyalarni himoyalash uchun blokcheyn keng qo‘llanmoqda. Blokcheyn texnologiyasi ham, xesh-funksiyalarning o'zi kriptografik nuqsonlarga ega bo'lishi mumkin va katta hajmdagi ma'lumotlarni boshqarish va tasdiqlash uchun juda ko'p vaqt sarflaydi. Bundan tashqari sun’iy intellekt (AI) va Mashinaviy o‘qitish (ML) asosidagi xavfsizlik tizimlari, jahon miqyosida kiberxavfsizlikda sun’iy intellekt va mashinaviy o‘qitish texnologiyalaridan keng foydalanilmoqda. Ushbu texnologiyalar kiberhujumlarni oldindan aniqlash, tahdidlarni avtomatik ravishda o‘rganish va g‘ayritabiiy xatti-harakatlarni kuzatish imkonini beradi.

MDH davlatlaridagi olimlardan Gleb Evstafiev(Rossiya) ning ishlari tarmoq xavfsizligi zaifliklarini aniqlashda katta samaradorlikka ega. U zaifliklarni aniqlashda o‘zgacha metodologiyani ishlab chiqib, avtomatlashtirilgan tahdidlarni aniqlash tizimlarini yaratgan. Ammo, tarmoqlarni xavfsizligini ta'minlashga qaratilganligi sababli, boshqa, masalan, individual qurilmalar yoki mobil tizimlarning xavfsizligi bilan kam shug‘ullanadi. Shuningdek, tizimning rivojlanishi uchun doimiy yangilanishlar zarur. Rinat Abdulin O‘zbekistonda davlat axborot tizimlari xavfsizligini ta'minlash uchun zaruriy xavfsizlik siyosatlarini ishlab chiqishga qaratilgan. Uning yondashuvi milliy talablarni inobatga olgan holda xavfsizlikni samarali ta’minlaydi. Biroq Abdulinda ham, asosan milliy xavfsizlik talablariga moslashganligi sababli, uning ishlari xalqaro xavfsizlik standartlariga to‘liq javob bermasligi mumkin. Shuningdek, ba’zi

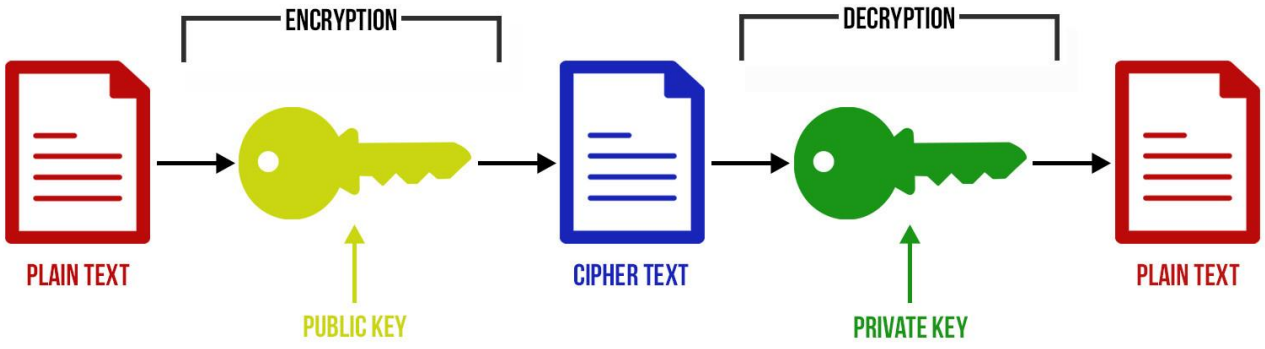
texnologiyalarni texnik vositalarsiz amalga oshirish qiyin bo‘lganligi sababli ba’zi kamchiliklar mavjuddir.

Tadqiqot metodologiyasi. Tadqiqotning asosiy maqsadi axborot xavfsizligini ta'minlashning zamonaviy usullari va texnologiyalarini o'rganish, tahlil qilish va amaliy misollar orqali samaradorligini baholashdir.

Tadqiqot jarayonida axborot xavfsizligini ta'minlash sohasida mavjud bo'lgan tadqiqotlar, ilmiy maqolalar va texnologik yechimlar tahlil qilindi.

Tahlil va natijalar. Axborot xavfsizligini ta’minlashda ko’plab usullardan biri RSA algoritmini ko’rib o’tamiz, RSA algoritmi katta tub sonlarni aniqlash, hisoblash jihatdan oddiy ekanligidan hamda shunday ikkita katta sonlarning ko’paytmasi bo’lgan sonni ko’paytuvchilarga ajratish judayam qiyin, amalda mumkin emasligidan foydalanishgan. RSA shifrini ochish shunday ko’paytuvchilarga ajratishga tengligi isbotlangan (Rabin teoremasi). Shuning uchun kalit uzunligi qanday bo’lishidan qat‘iy nazar shifrni ochish uchun talab qilinadigan amallarning quyi chegarasini baholash, zamonaviy kompyuterlarning tezligini bilgan holda shifrni ochish uchun kerak bo’ladigan vaqtni ham aniqlash mumkin.

RSA algoritmining himoyalanganlik kafolatini aniqlash imkoniyati, uning boshqa ochiq kalitli algoritmlar orasida mashhur bo’lishining sababi hisoblanadi. Shuning uchun RSA algoritmidan bank kompyuter tizimlarida foydalanilmoqda, ayniqsa uzoq masofadagi mijozlar bilan ishlashda (kredit kartochkalarga xizmat ko’rsatishda) qo’llanilmoqda. Quyida RSA algoritmining ishlash sxemasi kletirilgan:



1-rasm. RSA algoritmi

Algoritm, modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan. Algoritmni quyidagi qadamlar ketma-ketligi ko'rinishida ifodalash mumkin.

1-qadam. Ikkita 200 dan katta bo'lgan tub son **p** va **q** tanlanadi.

2-qadam. Kalitning ochiq tashkil etuvchisi **n** hosil qilinadi

n=p*q.

3-qadam. Quyidagi formula bo'yicha Eyler funktsiyasi hisoblanadi:

f(p,q)=(p-1)*(q-1). Eyler funktsiyasi **n** bilan o'zaro tub, **1** dan **n** gacha bo'lgan butun musbat sonlar sonini ko'rsatadi. O'zaro tub sonlar deganda **1** dan boshqa birorta umumiy bo'luvchisiga ega bo'lmagan sonlar tushuniladi.

4-qadam. f(p,q) qiymati bilan o'zaro tub bo'lgan katta tub son **d** tanlab olinadi.

5-qadam. Quyidagi shartni qanoatlantiruvchi **e** soni aniqlanadi

e*d mod f(p,q)=1 Bu shartga binoan ko'paytmaning **f(p,q)** funktsiyaga bo'lishdan qolgan qoldiq **1**ga teng. **e** soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi. Maxfiy kalit sifatida **d** va **n** sonlari ishlatiladi.

6-qadam. Dastlabki axborot uning fizik tabiatidan qat'iy nazar raqamli ikkili ko'rinishda ifodalanadi. Bitlar ketma-ketligi **L** bit uzunlikdagi bloklarga ajratiladi, bu yerda $\mathbf{L \geq \log_2 l}$ shartini qanoatlantiruvchi eng kichik butun son. Har bir blok **[0, n-1]** oraliqka taalluqli butun musbat son kabi ko'riladi. Shunday qilib, dastlabki axborot **X(i)**, **i=** sonlarning ketma-ketligi orqali ifodalanadi. **I** ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7-qadam. Shifrlangan axborot quyidagi formula bo'yicha aniqlanuvchi **Y(i)** sonlarning ketma-ketligi ko'rinishida olinadi:

Axborotni Deshifrlash qilishda quyidagi munosabatdan foydalaniladi:

X(i)=(Y(i))d (mod n).

Misol. "GAZ" so'zini shifrlash va deshifrlash qilish talab etilsin. Dastlabki so'zni shifrlash uchun quyidagi qadamlarni bajarish lozim.

1-qadam. **p=3** va **q=11** tanlab olinadi.

2-qadam. **n=p*q=33** hisoblanadi.

3-qadam. **f(p,q)=(p-1)*(q-1)=20** Eyler funktsiyasi aniqlanadi.

4-qadam. O'zaro tub son sifatida **d=3** soni tanlab olinadi.

5-qadam. **e*d mod f(p,q)=1** shartini qanoatlantiruvchi **e** soni tanlanadi. Aytaylik, **e=7**.

6-qadam. Dastlabki so'zning alfavitdagi xarflar tartib raqami ketma-ketligiga mos son ekvivalenti aniqlanadi. A xarfiga –1, G xarfiga -4, Z xarfiga –9. O'zbek alfavitida 36ta xarf ishlatilishi sababli ikkili kodda ifodalash uchun **6≥log236** ta ikkili xona kerak bo'ladi. Dastlabki axborot ikkili kodda quyidagi koэrinishga ega bo'ladi:

1-jadval

G	A	Z
000100	000001	001001

000100 000001 001001.

Blok uzunligi butun sonlar ichidan shartini qanoatlantiruvchi minimal son sifatida aniqlanadi. **L≥log$_2$33** bo'lganligi sababli **L=6**.

Demak, dastlabki matn ketma-ketlik ko'rinishida ifodalanadi.

7-qadam. Ketma-ketligi ochiq kalit {7,33} yordamida shifrlanadi:

Y(1)=(4^7 mod 33)=16384 mod 33=16

Y(2)=(1^7 mod 33)=1 mod 33 =1

Y(1)=(9^7 mod 33)=4782969 mod 33 =15

Shifrlangan so'z Y(i)=<16,1,15>

Shifrlangan so'zni Deshifrlash qilish maxfiy kalit **{3,33}** yordamida bajariladi.:

Y(1)=(16^3 mod 33)=4096 mod 33 =4

Y(1)=(13)(mod 33)=1 mod 33 =1

Y(1)=(153)(mod 33)=3375 mod 33 =9

Dastlabki son ketma-ketligi Deshifrlash qilingan **X(i)=<4,1,9>** ko’rinishida dastlabki matn bilan almashtiriladi. Natijada “GAZ” dastlabki matn hosil bo’ladi.

Xulosa va takliflar. Axborot xavfsizligi sohasida ko'plab olimlar o'zlarining ilmiy ishlari bilan katta hissa qo’shgan. Kriptografiya, tarmoq xavfsizligi, kiberhujumlarni aniqlash va oldini olish, hamda xavfsizlik protokollari bo’yicha ilmiy izlanishlar nafaqat ilm-fan, balki amaliy sohada ham katta ahamiyatga ega. Ularning ishlari bugungi kunda internet xavfsizligi va shaxsiy ma’lumotlarni himoya qilishda muhim rol o’ynamoqda. Yuqoridagi usullar jahon miqyosida kiberxavfsizlikda qo’llanilib, turli darajadagi axborot tizimlarini himoya qilishga yordam beradi. Har bir texnologiya va yondashuv o’ziga xos xavfsizlikni ta’minlab, ma’lumotlarning butunligini saqlash, ruxsatsiz kirishni cheklash va kiberhujumlarga qarshi kurashishga xizmat qiladi.

Bugungi globallashuv va raqamli texnologiyalar rivoji davrida axborot xavfsizligi dolzarb masalalardan biri bo‘lib qolmoqda. Har kuni yangi kiberhujumlar, ma’lumotlarning o‘g‘irlanishi yoki buzilish holatlari qayd etilmoqda. Shuning uchun axborot xavfsizligini ta’minlash texnologiyalarining rivoji va ularning samaradorligini oshirish masalalari jahon miqyosida muhim ahamiyat kasb etmoqda.

Mazkur maqolada, ishining maqsadi va uni yechish uchun oldinga qo‘yilgan vazifalar bo‘yicha axborot tizimlarida ma’lumotlarni saqlashda axborotlarni xavfsizligini ta’minlovchi algoritmi ishlab chiqildi hamda ishlab chiqilgan algoritm parametrga ko‘ra samaradorligini tasdiqlovchi natija olindi.

ADABIYOTLAR RO’YHATI

1. Axborot xavfsizligi asoslari [Matn] : o'quv qo'llanma / B.N. Tahirov .Buxoro: Fan va ta`lim, 2022 60-66.

2. G.H.To‘rayeva, D.H.Fayziyeva. / [Matn]: o‘quv qo‘llanma – Buxoro 2023. 5-21.

3. Gupta, A., & Sharman, R. (2022). *Cybersecurity in Cloud and IoT*. Journal of Information Security.

4. Singh, K., & Alam, M. (2023). *Advancements in AI-Based Cybersecurity*. International Journal of Cyber Defense.

5. Zaripova M.D., Boymatova D.O. Ta'lim sifatini baholashning Xorij tajribasi//Science, Research, Development.-2020.-T.25.-C.42-45.

6. Toyirov A.X., Zaripova M.J., Jumayev F.T. THE USE OF VIRTUAL COMPUTERS IN TEACHING OF INFORMATION DISCIPLINES //World science.- 2015.-T.1. - №.3(3). – C. 13-16

7. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. - New York, NY, USA: ACM, 1978. - T. 21. - № 2, Feb. 1978.

8. RFC 2631 – Diffie–Hellman Key Agreement Method E. Rescorla June 1999 - http://tools.ietf.org/html/rfc2631

9. Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory. — Nov. 1976. — T. IT-22.

10. Лапонина О.Р. Криптографические основы безопасности. — М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2004. — С. 320. — ISBN 5-9556-00020-5

Web manbalar

https://www.exabeam.com/explainers/information-security/information-security-goals-types-and-applications/

https://www.protectivesecurity.govt.nz/guidance/information-security/

https://www.tenable.com/principles/information-security-principles/