MAXSUS TARMOQLAR YORDAMIDA MA'LUMOTLARNI SHIFRLASH ALGORITMINI TAHLIL

Abduraximov B.F.
(O'ZMU professor fizika matematika fanlari doktori)
Murodqosimova SH.X.
(Muhammad Al-xorazimiy nomidagi TATU magistr)
Tursunov B.A.
(TDAU PhD mustaql tadqiqotchi)Toshkent davlat agrar universiteti "Raqamli ta'lim texnologiyalarini joriy etish va axborot xavfsizligini ta'minlash" bo'limi kontent menedjeri
Pochta manzil: b-tursunov87@mail.ru
https://doi.org/10.5281/zenodo.11221421

Annotasiya
Ushbu maqolada shifirlash algoritimni muammosi shifrlash algoritmini qanday maqsadlarga yo'naltirilishini va ma'lumotlarni xavfsizligi va tarmoq va tarmoqda bo'ladigan hujumlarga kriptobardoshligini aniqlash va malumot almashishdagi xavf-xatrlarni oldini olish chora tadbirlarini ishlab chiqishdan iborat Shu nuqtai nazardan, maqolada shifirlash algoritmlarini malumotlar xavfsizligini taminlashdagi bo'ladigan katta ahamiyatga ega , Bundan tashqari maqolamizda shifirlash algoritmalrini ko'rib tahlil qilib chiqamiz.
Kalit so'zlar: shifirlash algoritimni hujumlarga kriptobardoshligini aniqlash malumotlar xavfsizligini taminlashdagi tahlil.

Shifrlash algoritmini tarmoqlar yordamida tahlil qilishda, tarmoq xavfsizligi, ma'lumotlar himoyalash jarayonining to'liqligi va algoritmlarning ishlashini kuzatishning keng qamrovli o'rganilishi zarur. Bu, ma'lumotlarni o'g'irlash va maxfiylash jarayonida ma'lumotlarni xavfsizligini ta'minlash uchun muhimdir.

Maxsus tarmoqlar yordamida ma'lumotlarni shifrlash algoritmini tahlil qilish, xavfsizlik, darajasi, va qulayligi jihatidan muhimdir. Quyidagi asosiy nuqtalarni ko'rib chiqib o'tamiz:

1. **Maqsad va Talablar Tushunchasi**: Avval, shifrlash algoritmini qanday maqsadlarga yo'naltirilishini va qanday ma'lumotlarni qanday darajada himoyalashni talab qilayotganingizni aniqlash. Masalan, siz o'z ma'lumotlaringizni yolg'on ishlovchilardan himoyalashni talab qilayapsizmi, yoki siz sirli ma'lumotlarni o'z xodimlaringiz bilan ulashishda ishlatayotgan bo'lishingiz mumkin.
2. **Shifrlash Usullari Tanlash**: So'nggi kriptografiya texnologiyalari va protokollari to'g'risida ma'lumot olishingiz va ularni o'rganishingiz zarur. Bu, sizning maqsadingiz va talablaringizga mos ravishda ishlaydigan eng muhim shifrlash usulini tanlashda yordam beradi.
3. **Shifrlash Algoritmini ishlab chiqish**: Algoritmda ishlatiladigan asosiy mantiqiy va matematik jarayonlarni belgilang. Masalan, o'zgaruvchilarni almashtirish, shifrlash elementlarini birlashtirish va hokazo. Bu bosqichda, ushbu mantiqiy jarayonlarni muhim matematik formulalar yordamida ifodalovchi algoritmlarni yaratishingiz kerak.
4. **Test va Tahlil**: Yaratilgan algoritmani intensiv testdan o'tkazing. Bunda, turli ma'lumotlar toifalarini, qiziqarli holatlarni va taqiqlovchi ma'lumotlarni sinovdan o'tkazishingiz lozim. Bu, algoritmingizning to'g'ri ishlashi va xavfsizligini ta'minlash uchun juda muhimdir.
5. **Algoritmani Tahlil qilish va Yanada Rivojlantirish**: Algoritmingizni tahlil qilish va

uning ishlash jarayonini yaxshilash uchun yanada rivojlantirish uchun tushunchalarni qo‘llash va tarmoqdagi ma’lumotlar almashuvnidagi uzoq muddatdagi xavfsizlik va o‘tkazishni ta’minlash uchun juda muhimdir.

-Xavfsizlik: Maxsus tarmoqlar orqali ma'lumotlarni shifrlashda asosiy qaror - xavfsizlik. Algoritmlar shifrlash jarayonida ma'lumotlarni qanday darajada himoyalaydi, ma'lumotlar o'g'irishni qancha murakkablashtiradi va maxfiy kalitlar (key) nima sifatida saqlanadi bu nuqtalarda diqqatga sazovor bo'lish kerak.

-Analitik: Maxsus tarmoqlar uchun ma'lumotlarni shifrlash algoritmi hamda uning ulashish protokollari amalniylikni ta'minlashi zarur. Protokollar tarmoq xavfsizligi, yoritish, kalitlar o'zgarishini, ma'lumotlarni shifrlash va unshifrlashni amalga oshirish va boshqa kutiladigan xizmatlarni o'z ichiga oladi.

-Tezlik: Maxsus tarmoqlar orqali ma'lumotlarni shifrlashda tezlik juda muhimdir. Shifrlash va unshifrlash jarayonlari tarmoq trafikini cheklab turishi mumkinligi sababli tez vaqtning juda muhim qismini egallashi kerak.

-Kalitlar va kalit menedjmenti: Maxsus tarmoqlar uchun ma'lumotlarni shifrlashda maxfiy kalitlar juda muhimdir. Ularni sifatini, o'lchamini, hayot muddatini va o'zgarishlarni nazorat qilish uchun kalit menedjmenti muhimdir.

-Monitoring va o'zgartirish: Ma'lumotlarni shifrlash algoritmini amalga oshirishdan keyin monitoring tashkil etilishi zarur. Bu monitoring shifrlash algoritmining to'g'ri ishlashi, tarmoq trafikini tekshirish va xavfsizlik darajasini ta'minlash uchun juda muhimdir. Monitoring natijalariga asosan, algoritmlar va ulashish protokollari o'zgartirilishi mumkin.

-Tarqalgan xavfsizlik yechimlari: Xavfsizlik muammolarida osonlikka erishish uchun tarmoqda tarqalgan xavfsizlik yechimlari ham juda muhimdir. Shu bilan birga, maxsus tarmoqlar shifrlash uchun xavfsizligi oshirish uchun maxsus protokollar va xavfsizlik hodisalari mavjud bo'lishi kerak.

Bu elementlar maxsus tarmoqlar orqali ma'lumotlarni shifrlash algoritmini tahlil qilishda keng qamrovli o‘rganishni ta'minlaydi. Xavfsizlik, amalniylik, tezlik, va monitoring tarmoq xavfsizligini ta’minlash uchun juda muhim omildir.

Shifrlash yordamida ma’lumotlarni himoyalash – xavfsizlik muammolarining muhim yechimlaridan biri. Shifrlangan ma’lumotga faqatgina uni ochish usulini biladigan kishigina murojaat qilish imkoniga ega bo’ladi. Ruxsat etilmagan foydalanuvchi ma’lumotni o’g’irlashi hech qanday ma’noga ega emas. Kriptografik uslublarning axborotlar tizimi muhofazasida qo’llanishi ayniqsa hozirgi kunda faollashib bormoqda. Haqiqatan ham, bir tomondan kompyuter tizimlarida internet tarmoqlaridan foydalangan holda katta hajmdagi davlat va harbiy ahamiyatga ega bo’lgan hamda iqtisodiy, shaxsiy, shuningdek boshqa turdagi axborotlarni tez va sifatli uzatish va qabul qilish kengayib bormoqda. Ikkinchi tomondan esa bunday axborotlarning muhofazasini ta’minlash masalalari muhimlashib bormoqda.

Simmetrik shifrlash algoritmi - bu ma’lumot yoki xabarni shifrlash va keyin shifrlash uchun bitta kalitdan foydalanadigan shifrlash usuli. Bu maxfiy yoki shaxsiy kalit bo’lgani uchun, simmetrik shifrlash algoritmlaridan foydalangan holda muloqot qilayotgan tomonlar kalitni xavfsiz almashishlari kerak. Simmetrik shifrlash algoritmlari assimetrik shifrlash algoritmlaridan keskin farq qiladi, ular bitta shaxsiy kalit va ma’lumotni shifrlash va keyin shifrini ochish uchun bitta ochiq kalitdan foydalanishga tayanadi.

Umuman olganda, bu simmetrik va assimetrik shifrlash algoritmlari o’rtasidagi farqlarni tavsiflaydi:

- Simmetrik kalitlarni shifrlash algoritmlari kalit uzunligi 128 yoki 256 bitga ega. Asimmetrik shifrlash algoritmlari kalit uzunligi 2048 (RSA) yoki undan yuqori.
- Simmetrik shifrlash algoritmlariga AES, DES, 3DES va RC4 kiradi. Asimmetrik shifrlashdan foydalanadigan algoritmlar RSA va Diffie-Hellmandir.

XULOSA

Axborot texnologiyalarining hozirgi zamon taraqqiyoti hamda yutuqlari fan va inson faoliyatining barcha sohalarini axborotlashtirish zarurligini taqozo etmoqda. Chunki aynan mana shu narsa butun jamiyatning axborotlashtirilishi uchun asos va muhim zamin bo‘ladi. Jamiyatni axborotlashtirish respublikamiz xalqi turmush darajasining yaxshilanishiga, ijtimoiy ehtiyojlarning qondirlishiga, iqtisodning o‘sishi hamda fan-texnika taraqqiyotining jadallashishiga xizmat qiladi.

References:

1. www. intuit.ru
2. www. ziyonet.uz
3. www. nuu.uz
4. www. tuit.uz
5. www.rsa.com
6. Martin E. Hellman An overview of public key cryptography
7. www.comsoc.org/livepub.s/cil/public/anniv/pdfs/hellman.pdf
8. www.williamspublishing.com/PDF/5-8459-0847-7/part.pdf
9. www. security.uz
10. www. cert.uz
11. www. unicon.uz
12. www. uzinfocom.uz
13. http://ccitt.uz/ru
14. www. securitylab.ru
15. www.wikipedia.org
16. www. cryptopro.ru
17. www.itsecurity.com
18. www.securityfocus.com
19. www. cert.org
20. www.infosyssec.com
21. www. securit.ru
22. www.leta.ru
23. www. cryptobook.rsu.ru
24. www.nasa.gov \statistics\