AXBOROTLARNI HIMOYALASHDA AES KRIPTOGRAFIK ALGORITMINING IMKONIYATLARI

Seytniyazov Davronbek Bayramovich *tayanch doktorant*
Atamuratova Shaxsanem Turdimuratovna *talaba*
Dauletmuratova Juldiz Ayapbergenovna *talaba*
Jumaniyazova Ulbosin Polatbay qizi *talaba*

Bugungi kunda axborotlashgan jamiyat jadal suratlar bilan shakllanib, axborotlar dunyosida davlat chegaralari degan tushuncha yo'qolib bormoqda. Global kompyuter tarmog'i jahon davlatlarining ijtimoiy-iqtisodiy, siyosiy, ma'naviy va madaniy hayotida alohida ahamiyat kasb etmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi bo'lib hisoblanadi. O'zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimini yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o'z ifodasini topdi. Bu borada O'zbekiston Respublikasining «Davlat sirlarini saqlash to'g'risida»gi, «Axborotlashtirish to'g'risida»gi va boshqa qonunlar qabul qilindi hamda amalda tatbiq etib kelinmoqda.

Axborot xavfsizligi - bu axborotning saqlanishi va himoya qilinishini ta'minlashga, shuningdek unga ruxsatsiz kirishning oldini olishga va uning egasiga zarar yetkazishga qaratilgan chora-tadbirlar majmuidir. Zamonaviy dunyoda ushbu mavzuning dolzarbligi shubhasizdir, chunki axborot texnologiyalari va kommunikatsiyalari odamlarning kundalik hayotida, shuningdek, korxonalar, tashkilotlar va davlatlar faoliyatida tobora muhim rol o'ynamoqda.

Hozirda axborotlarni himoyalashda eng keng qo'llaniladigan usullarning biri bu shifrlash bo'lib uni amalga oshirishda birnechta algoritmlardan foydalanilmoqda. Shu kabi algoritmlardan biri AES shifrlash algoritmi bo'lib hisoblanadi.

Kengaytirilgan shifrlash standarti (AES) algoritmi dunyodagi eng keng tarqalgan simmetrik ma'lumotlarni shifrlash algoritmlaridan biri bo'lib hisoblanadi. Bu algoritm 2001 yilda AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan va avvalgi shifrlash standarti DES algoritmini o'rniga foydalanish uchun taqdim etilgan.

AES axborotlarni uzatish yoki saqlashdan oldin ularni shifrlash orqali ma'lumotlarning maxfiyligi va yaxlitligini himoya qilish uchun ishlatiladi. U turli sohalarda, jumladan, axborot xavfsizligi, moliya, tibbiyot, hukumat va hatto shifrlangan flesh-disklar va Wi-Fi routerlar kabi iste'molchi ilovalarida keng qo'llaniladi.

AES bitni almashtirish va aralashtirish printsipi asosida ishlaydi. U 128-bitli ma'lumotlar bloklarini shifrlash uchun 128, 192 yoki 256-bitli kalitdan foydalanadi. AES bir nechta qadamlardan iborat bo'lib, ularning har birida quyidagi operatsiyalar amalga oshiriladi:

1. SubBytes: ma’lumotlar blokidagi har bir baytni oldindan belgilangan S Box almashtirish jadvalidagi mos keladigan element bilan almashtiradi.

2. ShiftRows: ma’lumotlar blokining har bir qatorini ma’lum bir bayt soniga siklik ravishda chapga siljitadi.

3. MixColumns: ma’lum bir ko’paytirish matritsasi yordamida ma’lumotlar blokining har bir ustunini o’zgartiradi.

4. AddRoundKey: XOR operatsiyasini ma’lumotlar bloki va yashirin kalit o’rtasida qo’llaydi.

AES-dagi har bir qadam AddRoundKey operatsiyasi bilan tugaydi. Birinchi qadamda kalit asosiy kalitning birinchi 128 bitiga teng bo’ladi, keyingi qadamlarda esa oldingi kalit asosida hisoblab chiqiladi.

Ma’lumotlarni himoya qilish uchun shifrlash kaliti ishlatiladi, uning uzunligi 128, 192 yoki 256 bit bo’lishi kerak. Kalit xavfsiz tarzda yaratilishi, xavfsiz joyda saqlanishi va faqat shifrlangan tarzda uzatilishi kerak.

AES brut force, chiziqli va differentsial kriptoanaliz hujumlari kabi turli hujumlarga chidamliligi tufayli yuqori darajadagi xavfsizlikni ta’minlaydi. Shuningdek, u parallel ishlov berishni qo’llab-quvvatlaydi, bu uni ko’p yadroli protsessorlar va bulutli hisoblash uchun samarali qiladi.

AES shuningdek, yuqori unumdorlik va kam resurs xarajatlariga ega bo’lib, uni keng ko’lamli ilovalarda, jumladan, mobil qurilmalar va o’rnatilgan tizimlarda ishlatish imkonini beradi. Ommabopligi tufayli AES ko’plab dasturlash tillari va kutubxonalarida, jumladan C#, Python, Java va boshqa ko’plab dasturlarda keng qo’llab-quvvatlanadi.

AES ning asosiy afzalliklaridan biri bu algoritmning turli xil amalga oshirishlari o’rtasidagi muvofiqlikni ta’minlaydigan standartlashtirishdir. Bu shuningdek, agar to’g’ri kalit ma’lum bo’lsa, AES shifrlangan ma’lumotlarning boshqa har qanday AES ilovasi yordamida shifrlanishi mumkinligini anglatadi.

Barcha afzalliklarga qaramay, AES ba’zi kamchiliklarga ega. Misol uchun, u xabarning autentifikatsiyasini ta’minlamaydi, ya’ni tajovuzkor shifrlangan ma’lumotlarni parolini ochish kalitiga ega bo’lmasdan o’zgartirishga urinishi mumkin. Bunday hujumlardan himoya qilish uchun AES ko’pincha HMAC yoki RSA kabi xabarlarni autentifikatsiya qilish algoritmlari bilan birgalikda ishlatiladi.

AES ning yana bir kamchiligi - u qayta ishlay oladigan ma’lumotlar blokining hajmi. AES 128 bitli ma’lumotlar bloklari bilan ishlaydi, bu oqimli shifrlash yoki katta fayllarni shifrlash kabi ba’zi ilovalar uchun yetarli bo’lmasligi mumkin. Biroq, ma’lumotlarni kattaroq bloklarda qayta ishlashga imkon beruvchi blok zanjiri (CBC) yoki gamut teskari aloqasi (OFB) kabi shifrlash rejimlari yordamida bu kamchilikni bartaraf etish mumkin.

Yuqorida keltirilgan kamchiliklari borligi algoritmning ishonchliligini kamaytirmaydi shuning uchun ham mazkur algotirm juda ko’plab sohalarda qo’llaniladi.

Xulosa qilib aytadigan bo’lsak AES hozirda mavjud bo’lgan eng xavfsiz va keng qo’llaniladigan ma’lumotlarni shifrlash algoritmlaridan biri bo’lib hisoblanadi. U yuqori darajadagi xavfsizlik, ishlash va standartlashtirishni ta’minlaydi, bu esa uni konfidensial ma’lumotlarni himoya qilishni talab qiladigan ko’pgina ilovalar uchun ideal tanlov qiladi. Biroq, AES-dan foydalanganda, barcha cheklovlarni hisobga olishimiz va maksimal ma’lumotlar xavfsizligini ta’minlash uchun to’g’ri kalit hajmini, shifrlash rejimlarini va xabarni autentifikatsiya qilish algoritmlarini tanlashimiz kerak.

FOYDALANILGAN ADABIYOTLAR:

1. Каримов И.М., Тургунов Н.А., Кадиров Ф., Самаров Х.К., Иминов А.А., Джаматов М.Х. Ахборот хавфсизлиги асослари: Маърузалар курси. – Т., 2013.
2. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособ. – М.: Гелиос АРВ, 2005.
3. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М., 2000.