Proceedings of International Conference on Educational Discoveries and Humanities
Hosted online from Plano, Texas, USA.
Date: 1st February, 2023
ISSN: 2835-3196 **Website:** econferenceseries.com

AES SHIFRLASH ALGORITMINING O`ZIGA XOSLIGI

Alimov Davronbek G'ulom o'g'li
Mirzo Ulug`bek nomidagi O`zbekiston Milliy universiteti magistranti

Annotatsiya:
Ushbu maqolada rivojlangan mamlakatlarda keng foydalaniladigan va ma'lumotlarni shifrlashda va uzatishda samarali bo`lgan algoritmlardan biri AESS shifrlash algoritmi haqida ma'lumot berilgan.

Kalit so'zlar: AES, DES, FIPS, CUI, SSD, SED, Google Cloud, MozillaFirefox, Opera, Rijndael algoritmi, oltin standart.

KIRISH

Qadimgi shifrlash uslublari har-xil jadvallarga asoslangan bo`lib, bu jadvallar ma'lumotlar matnidagi alfavit belgilarining ma'lum tartibdagi o`rin almashtirishlarini ifodalovchi oddiy amallardan iborat bo`lgan. Bunda kalit vazifasini jadvalning o`lchami, alfavit belgilarining almashtirilishini taminlovchi biror aniq jumla yoki jadvalning o`rin almashtirishlarini tartiblovchi alohidalik xususiyati va shu kabilar o`tagan.

ADABIYOTLAR SHARHI

DES blokli shifrlash algoritmi 1999 yilgacha AQShda standart shifrlash algoritmlari sifatida ishlatib kelingan.
1974 yildan Amerika qo'shma shtatlarining standart shifrlash algoritmisifatida qabul qilingan DES shifrlash algoritmi quyidagi:

- kalit uzunligining kichigligi (56 bit);

S-blok akslantirishlarining differensial kriptotahlil usuliga bardoshsizligi; va boshqa sabablarga ko'ra eskirgan deb sanaladi. Ayniqsa 1999 yilda DES shifrlash algoritmi yordamida shifrlangan ma'lumotning Internet tarmog`igaulangan 300 ta parallel kompyuter tomonidan yigirma to`rt soat davomida ochilishi haqidagi ma'lumotning tasdiqlanishi bundan keyin mazkur standart algoritmiyordamida ma'lumotlarni kriptografik muhofaza qilish masalasini qaytadan ko`ribchiqish va yangi standart qabul qilish zaruratini keltirib chiqardi va yangi shifrlashalgoritmiga ehtiyoj kundan-kunga ortdi.

TADQIQOT METODOLOGIYASI VA EMPIRIK TAHLIL

AES(Advanced Encryption Standard) - NIST tomonidan chiqarilgan va shu bilan birga 1996 yildagi “Axborot texnologiyalarini boshqarish islohoti to`g`risida”gi qonun va 1987 yildagi “Kompyuter xavfsizligi to`g`risida”gi qonun bilan qonuniy muvofiqligini ta’minlash uchun AQSH Savdo vaziri tomonidan nashr etilishidan oldin ma’qullangan ko`plab federal ma’lumotlarni qayta ishlash standartlaridan (**FIPS**) bir hisoblanadi. Bu standart AQSH oldingi standarti DES o`rniga ishlatilyapti. Maxfiy va o`ta maxfiy ma’lumotlar va razvedka ma’lumotlarini uzatish va shifrlash uchun Milliy xavfsizlik agentligi (NSA) tomonidan tasdiqlangan yagona ommaviy blokli shifrdir . Morris Dvorkin, Eleyn Barker, Jeyms Nechvatal, Jeyms Foti, Lourens Bassam, Edvard Robek va kichik Jeyms Dray mualliflik qilgan AES 2001-yil 26-noyabrda nashr etilgan va 2002-yildaAQSh hukumati tomonidan qabul qilingan. Xususan AES algoritmi **Rijndael** nomibilan ham tanilgan va Belgiya kriptograflari Vinsent Rijmen va Joan Daemen tomonidan ishlab chiqilgan Rijndael shifrlash algoritmlari oilasidan olingan.

Ma'lumki, AES algoritmini hali hech bo`lmaganda bir umr davomida buzish mumkin emas. Bu olishini milliardlab , hatto **128 bit** AES kalit yorilish bir kompyuter uchun ko`p yil yoki milliardlab yillarni talab qiladi.

Kvant kompyuterlari AES algoritmlarini tezroq buzishi mumkin, ammo ba’zi manbaalarga ko’ra, kvant kompyuteriga 128 bitli AES kalitining imkoniyatlarini to`ldirish uchun taxminan olti oy kerak bo'ladi. Nashr qilingan kundan boshlab, AES algoritmlari shafqatsiz kuchlar hujumlariga virtual o`tib bo`lmasligi tufayli butun dunyo bo`ylab elektron ma’lumotlarga, shu jumladan nozik ma’lumotlarga, boshqariladigan maxfiy ma’lumotlarga ruxsatsiz kirishni xavfsiz shifrlash va oldini olish uchun kriptografik **oltin standart**ga aylandi. Federal hukumat idoralari, shuningdek, nodavlat, notijorat tashkilotlar va korxonalari o`zlarining maxfiy ma’lumotlarini himoya qilish uchun har kuni AES shifrlashdan foydalanadilar. Hatto iste’molchilar ham, ko`pincha o`zlari bilmagan holda, AES shifrlashni amalga oshiradigan qurilmalardan foydalanadiladi.

Federal hukumat nazorat ostidagi tasniflanmagan ma'lumotlar (CUI) va maxfiy ma'lumotlar kabi maxfiy ma’lumotlar AES algoritmidan foydalangan holda kriptografik himoyaga kafolat beradimi yoki yo'qligini aniqlash uchun jarayonlarga ega, ammo AES shifrlash iste'molchi darajasidagi qurilmalar, ilovalar va boshqalarda ham qo'llaniladi va tarmoqlar, jumladan qattiq holatdagi drayvlar **SSD**),

o`z-o`zini shifrlaydigan drayvlar (**SED**), **Google Cloud** xotirasi, **Mozilla Firefox** va **Opera** kabi internet brauzerlari va veb-sayt xavfsizlik sertifikatlari tashkil etadi. Foydalanuvchilar NISTning Kompyuter xavfsizligi resurs markazigakirish , “FIPS” tugmasini bosish va “FIPS 197” ga o‘tish orqali AES nusxasini yuklab olishlari mumkin. AES hamma uchun ochiq ma’lumotdir, shuning uchun unga kirish uchun hech qanday to`lov olinmaydi. NIST ham AES-ni o'rganayotgan raqiblar bilan unchalik tashvishlanmaydi, chunki hozirgi texnologiyadan foydalanib uni buzish mumkin emas.

XULOSA VA MUNOZARA

Bu standart boshqa standartlarga qaraganda o`zining kriptoturg`unligi bilan ajralib turadi. Unda foydalanilgan matematik amallarning murakkablik darajasi uning turg`unligini yanada oshiradi. Chunki bu algaritimda shifrlangan ma`lumotlar hujumlarga bardoshliligi yuqori.

ADABIYOTLAR RO`YXATI

1. Nil’s Fergyuson, Bryus SHnayer «Практичскя криптография», 2015yil.
2. Petrov A.A. «Компютерная безопасностъ. Криптографичиске методи zащити», M.: DMK, 2010 yil.
3. Shnayer Bryus. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnыe tekstы na yazыke Si. Triumf. 2012.
4. Barichev S. V. Kriptografiya bez sekretov. –M.: Nauka, 2018.