SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARINING O`ZIGA XOSLIGI

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

Annotatsiya: S-box-dan foydalanish zamonaviy kriptografiyada qo'llaniladigan ko'plab simmetrik blokli shifrlash algoritmlarining muhim tarkibiy qismidir. Shu bilan birga, turli kriptoanaliz usullariga qarshi tura oladigan mustahkam S-bloklarini yaratish murakkab muammodir. Ushbu maqolada biz S-bloklarni loyihalashda tasodifiylik va nochiziqlilikka erishish muammolarini va xavfsizlikni ta'minlash uchun ushbu bloklarning ko'p sonini yaratish muammolarini tasvirlab beramiz.

Kalit so‘zlar: Simmetrik shifrlash algoritmlari, blokli shifrlash, S-blok, P-blok, kriptografiya, generatsiya, nochiziqlilik.

KIRISH

Zamonaviy kriptografiyada blokli shifrlash axborot xavfsizligini ta’minlovchi algoritmlarning muhim tarkibiy qismidir, chunki u maxfiy kalit bilan shifrlash orqali ma'lumotlarning maxfiyligi va yaxlitligini ta'minlaydi.

Simmetrik blokli shifrlash - ma'lumotlarning ma’lum bir bitli uzunlikdagi bloklarida ishlaydigan shifrlash algoritmining turidir. Ochiq matn belgilangan o'lchamdagi bloklarga bo'linadi va shifrlash algoritmi maxfiy kalit yordamida har bir bloklarda shifrlanadi. Shifrlash algoritm orqali chiquvchi natija berilgan ochiq matn bilan bir xil uzunlikka ega bo'lgan shifrmatndir.

Blok shifrlash shifrlari yuqori darajadagi xavfsizlikni ta'minlaydi va xavfsiz aloqa, elektronbank va raqamli imzolar kabi ko'plab kriptografik ilovalarda qo'llaniladi. Eng keng tarqalgan blokli shifrlash shifrlaridan ba'zilari AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard).

ADABIYOTLAR SHARHI

AES shifrlash simmetrik kalitli shifrlash algoritmi bo'lib, u 128 bit blok o'lchamidan foydalanadi va 128, 192 yoki 256 bit uzunlikdagi kalitlarni qo'llab-quvvatlaydi. U simsiz xavfsizlik, elektron to'lov tizimlari va VPN kabi ko'plab ilovalarda keng qo'llaniladi.

DES shifrlash simmetrik kalitli shifrlashning yana bir algoritmi bo'lib, blok o'lchami 64 bit va kalit o'lchami 56 bitdan iborat. U ko'p yillar davomida keng qo'llanilgan, ammo hozirda kalit uzunligi qisqa bo'lgani uchun xavfli hisoblanadi.

3DES shifrlash DESga nisbatan takomillashtirildi va algoritm xavfsizligini oshirish uchunshifrlashning uch bosqichidan foydalanadi. U 64 bitli blok o'lchamidan

va 168 bitli kalit hajmidan foydalanadi, bu DESga qaraganda yuqori darajadagi xavfsizlikni ta'minlaydi.

Blok shifrlash shifrlari ma'lumotlarning maxfiyligi, yaxlitligi va haqiqiyligini ta'minlash uchun mo'ljallangan. Ular bunga almashtirish, almashtirish va diffuziya kabi turli usullardan foydalanish orqali erishadilar. O'zgartirish - almashtirish jadvali yordamida ochiq matnni shifrlangan matn bilan almashtirishni o'z ichiga oladi, almashtirish esa ochiq matnning bitlarini qayta tartibga solishni o'z ichiga oladi. Diffuziya ochiq matnning bir bitining ta'sirini shifrlangan matnning ko'p bitlariga tarqatishni o'z ichiga oladi.

TADQIQOT METODOLOGIYASI VA EMPIRIK TAHLIL

Kriptobardoshli shifrlash algoritmlarni ishlab chiqishda uning asosiy qismlaridan biri chiziqsiz akslantirishdan iborat S-blok muhim hisoblanadi. S-blok Feystel yoki SP tarmoqqa asoslangan simmetrik shifrlash algoritmlar standartlarida keng qo‘llaniladi [1,2]. Bardoshli kriptografik algoritmlarni loyihalashda kuchli S-blok ochiq matnning shifrmatn bo‘ylab yaxshi diffuziyasini ta’minlaydi, bu ochiq matn va shifrlangan matn o‘rtasidagi munosabatni aniqlashni qiyinlashtiradi. Shifrlash algoritmlarini ishlab chiqishda statik va dinamik S-bloklardan foydalaniladi.

Blokli shifrlashning asosiy operatsiyasi nochiziq akslantirish qiymatlari (S-blok) va chiziqli akslantirish qiymatlari (P-blok) dan iborat bo'lgan almashtirish-o'zgartirish tarmog'i (SP tarmoq) yoki Feystel tarmog’iga asoslangan shifrlash algoritmlarda ishlatiladi. S-blok har bir kirish bitlari qiymatini mos keladigan chiqish qiymatga chiziqsiz almashtiradi, P-blok esa S- blokldan chiquvchi qiymatlarini chiziqli akslantirish orqali aralashtirib yuboradi. Mazkur jarayonlarning kombinatsiyasi kiruvchi ochiqmatn va kalit bitlarini shifrmatn bo’ylab chalkashishini va tarqalishni ta'minlaydi. Bu esa tajovuzkorlarga shifrlangan matnni tahlil qilishni va ochiq matnni tiklashni qiyinlashtiradi.

Bardoshli S-bloklarni loyihalash muammolari.

Blokli shifrlash standartlari uchun bardoshli S-blok loyihalash ilmiy tomonlama qiyin vazifalardan biri hisoblanadi. Zaif S-bloklar shifrlash algoritmlari uchun xavfsizlik muammolarini keltirib chiqarishi mumkin. Agar S-blok turli mezonlarga asoslangan holda ishlab chiqilmagan bo'lsa, u differentsial kriptoanaliz, chiziqli kriptotahlil va algebraik kriptotahlil kabi turli xil hujumlarga bardosh bera olmasligi mumkin. Shuning uchun, hujumlar va tahlillarga bardoshli S- bloklarni loyihalash blokli shifrlash algoritmlarining xavfsizligi uchun juda muhimdir. Bardoshli S-bloklarni ishlab chiqarishda yuzaga keladigan ba'zi muammolar:

Xavfsizlik: S-bloklarni loyihalashda asosiy masala ularning hujumlarga qarshi xavfsizligini ta'minlashdir. S-bloklarning differentsial kriptotahlil, chiziqli kriptoanaliz va qo'pol kuch hujumlari kabi turli xil hujumlarga chidamliligini ta'minlash muhimdir.

Statistik xususiyatlar: S-bloklar chiqishda noaniqliklarga yo'l qo'ymaslik uchun

yaxshi statistik xususiyatlarga ega bo'lishi kerak. S-bloklar chiqish qiymatlarining bir xil taqsimlanishigaega bo'lishi kerak va ularning chiqishi kirishdan mustaqil bo'lishi kerak. Agar chiqish kirishdan mustaqil bo'lmasa, tajovuzkor kalit yoki ochiq matn haqida ma'lumot olish uchun undan foydalanishi mumkin.

Tezlik: S-bloklar tez va samarali bo'lishi uchun mo'ljallangan bo'lishi kerak. Sekin S- bloklar butun shifrlash tizimining ishlashiga ta'sir qilishi mumkin.

Chidamlilik: S-bloklar bardoshli bo'lishi va uzoq vaqt davomida hujumlarga qarshi turishiuchun mo'ljallangan bo'lishi kerak. Agar S-bloklar bardoshli bo'lmasa, tajovuzkor shifrlash tizimini buzish uchun S-bloklardagi zaif tomonlardan foydalanishi mumkin.

Kriptografik kalitlarni boshqarish: S-bloklar odatda kriptografik kalitlarni boshqarish usullari yordamida yaratiladi. Shuning uchun S-bloklarining xavfsizligi kalitlarni boshqarish tizimining xavfsizligiga bog'liq. Kalitlarni boshqarish tizimidagi har qanday zaifliklar S-bloklari va butun shifrlash tizimining xavfsizligini buzishi mumkin.

S-bloklar kirish(bit)ini chiqish(bit)iga nochiziqli bo’lishini ta’minlash uchun mo'ljallangan, ya'ni S-blokining chiqish(bit)i kirish(bit)ning chiziqli funktsiyasi sifatida ifodalanishi mumkin emas. Agar S-blok chiziqli bo'lsa, u butun shifrlash algoritmining xavfsizligini buzishi mumkin bo'lgan chiziqli kriptoanaliz yordamida osongina hujum qilinishi mumkin.

XULOSA VA MUNOZARA

S-box-ni ishlab chiqish usulini tanlash kriptografik algoritmning o'ziga xos talablariga va zarur bo'lgan xavfsizlik darajasiga bog'liq. Har bir yondashuvning o'ziga xos afzalliklari va kamchilliklari mavjud bo’lib eng yaxshi yondashuv usullarda amalga oshiriladigan kombinatsiyalardan kelib chiqqan holda tanlash mumkin. Umuman olganda, yuqori darajadagi xavfsizlikni ta'minlaydigan usullar hisoblash quvvatlari qimmat va keng masshtabdagi hisoblashnitalab qilgani uchun ancha qiyindir, amalga oshirish osonroq bo'lgan algoritmlarning esa xavfsizlik darajasi pastroq bo'lishidir. Shu sababli, umumiy kriptografik tizimning samaradorligini ta'minlash uchun hosil bo'lgan S-bloklarning xavfsizligini sinchkovlik bilan baholash va tahlil qilish juda muhimdir.

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. Рахматов, З. Н., & Рашидов, Д. Н. (2023). Пути совершенствования механизма разработки маркетинговой стратегии ао «ўзтемирйўлйўловчи». *Innovative achievements in science 2022*, *2*(17), 55-60.

5. Barichev S. V. Kriptografiya bez sekretov. –M.: Nauka, 2018.