ASIMMETRIK SHIFRLASH ALGORITMLARIGA AKTIV KRIPTOHUJUM USULLARI QO'LLANISHLARI

Babajonov Ma'mur Maxsudovich

Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti

"Amaliy matematika va inkellektual texnologiyalar" fakulteti

"Kripotografiya va kriptoanaliz" yo'nalishi 2-bosqich magistranti.

E-mail: babajonovmamur98@gmail.com

ANNOTATSIYA

Asimmetrik shifrlash algoritmlariga aktiv kriptohujum, passiv hujum usuli qo'llanishi bayon qilingan.

Kalit so'zlar: Passiv hujum, shifrlash, Aktiv hujum, algoritm, logarifmlash, yopiq kalit.

Bugungi kunda zamonaviy asimmetrik algoritmlar bardoshligi simmetrik shifrlar bardoshligidan farqli ravishda ma'lum matematik masalalarga asoslanadi. Jumladan matematik murakkablik asoslari sifatida berilgan sonni tub ko'paytuvchilarga ajratish (faktorizatsiya) va chekli maydonda diskret logarifmlash masalalari e'tirof etiladi.

Oxirgi o'ttiz yillik – kriptologiyaning barcha masalalari bo'yicha ilmiy ishlarning juda jadal o'sishi bilan xarakterlanadi. Kriptologiyaning kriptotahlil yo'nalishi esa faol rivojlanayotgan tadqiqot sohasi hisoblanadi.

Axborot texnologiyalarining rivojlanishi, hisoblash qurilmalarining takomillashuvi hamda kriptotahlil usullarining yutuqlari standart shifrlash algoritmlari asosida yaratilgan va kriptobardoshli deb hisoblangan ayrim kriptotizimlar bardoshliligi bahosini katta savol ostiga qo'ilishiga sabab bo'lmokda.

Telekommunikatsiya tarmog'ida shifrlangan ma'lumotni uzatish jarayonida kriptoanalitik: passiv yoki aktiv hujum turlarini amalga oshiradi.

Passiv hujum – maxfiy ma'lumotni aloqa tarmog'ida uzatilayotganda eshitish, taxlil qilish, yozib olish kabi hatti-harakatlardan iborat bo'lib, uzatilayotgan ma'lumot qabul qiluvchiga o'zgarishsiz yetib boradi.

Aktiv hujum – maxfiy ma'lumot uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash kabi hatti- harakatlardan iborat.

Bugungi kunda zamonaviy asimmetrik kriptografiya fanida "Tanlab olingan ochiq matn asosidagi hujum(chosen-plaintext attack-CPA)", "Tanlab olingan shifr matn asosidagi hujum(chosen-ciphertext attack-CCA)", "Adaptiv tanlab olingan shifr matnlar asosidagi hujum (adaptive chosen- ciphrtext attack-CCA2)" kabi aktiv kriptohujum usullaridan kelib chiqib, asimmetrik kriptotizimlar bardoshli bo'lishi uchun asosiy talablar ishlab chiqilgan. Ular bo'yicha tahliliy ma'lumot keltirilgan.

O'tkazilgan tahlil natijalariga ko'ra quyidagi tasdiq o'rinli. RSA standart algoritmi aktiv kriptohujum usuliga bardoshsiz.

Shuning uchun mazkur asimmetrik algoritmni amaliyotda klassikadabiyotlarda keltirilgan qadamlarida foydalanilishi maqsadga muvofiq emas.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. Akbarov D. E. "Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi" – Toshkent, 2008

2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.[уточнить]

3. Б. А. Фороузан. Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.

4. http://www.hozir.org/el-gamal-shifrlash-algoritmi.html