KRIPTOGRAFIK KALIT ALMASHINUVIDA NEYRON TARMOQ TEXNOLOGIYASIDAN FOYDALANISH

Allanov Orif Menglimuratovich
TATU, Kiberxavfsizlik va kriminalistika kafedrasi mudiri, phd.
E-mail: orif_allanov@mail.ru

Saparbayeva Munira Muratbay qizi
TATU magistranti

ANNOTATSIYA

Ushbu maqolada sun’iy neyron tarmoqlaridan foydalanib yuqori kalitlarni almashish usuli tadqiq etilgan.

Kalit so‘zlar: Kriptografiya, neyron tarmoq, sun’iy neyron, tarmoq, daraxt, kalit, kalit, kriptologiya, kriptoanaliz.

Kriptografiya muhim soha bo‘lib, ko‘plab ijtimoiy tarmoqlar va ilovalarda qo‘llaniladi. Ayni paytda shifrlash va autentifikatsiya texnologiyalari butun dunyo bo‘ylab xavfsizlik, harbiy va mudofaadan tortib elektron tijorat va bank ishi kabi davlat xizmatlarigacha borgan sari ko‘proq foydalanilmoqda.

Kiberhujum atamasi tobora ommalashib borayotganligi sababli, ma’lumotlarning maxfiyligi ko‘plab axborot xavfsizligi sohasidagi mutaxassislarni tashvishga solmoqda. Muammoni hal qilish uchun ushbu tadqiqotda kriptografiya maxfiy ma’lumotlarni himoya qilish vositasi sifatida kiritilgan, chunki u ochiq matnni begona shaxslar tomonidan o‘qib bo‘lmaydigan va tushunarsiz shifrlangan matnga aylantiradi [2].

Kriptografiya nazariyasi nafaqat axborotni shifrlash va deshifrlash, balki boshqa muammolarni hal qilish uchun ham qo‘llaniladi. Ma’lumot manbaasini autentifikatsiya qilish (elektron imzo texnikasi), kalit egasini sertifikatlash (ochiq kalit sertifikati), va xavfsiz elektron tranzaktsiyalar. Kriptografik tadqiqotlar natijalari, masalan, onlayn so‘rov dasturlari, masofaviy o‘qitish ilovalari va xavfsizlikni boshqarish ilovalari kabi haqiqiy ilovalarning murakkab ehtiyojlarini qondirish uchun boshqa usullar bilan birlashtirilgan[1].

Kriptografik amaliyotning zaif tomoni ham bor, ya’ni qabul qiluvchida shifrlangan matnni ochish uchun jo‘natuvchining maxfiy kaliti bo‘lishi kerak. Ushbu zaiflikni tan olgan holda, tajovuzkorlar maxfiy kalit almashinuv jarayonini nishonga olishadi, chunki bu kriptografik amaliyotdagi eng zaif bo‘g‘inlardan biridir.

Kriptografiyaning birinchi ixtiro qilingan kalit almashinuvi tizimi Diffie Hellman kalit almashinuvidir. Bu algoritm ikki abonent o‘rtasida kalitlarni almashish uchun eng ko‘p ishlatiladi. Kalit almashinuvi tizimi har ikki tomon (shaxs va aloqa ob’ekti) himoyalanmagan aloqa tarmoqlarida foydalaniladigan ma’lumotlarni shifrlash uchun umumiy maxfiy kalitni yaratish imkonini beradi, bunda ikki tomon o‘rtasida maxfiy kalit bo‘yicha oldindan kelishuv bo‘lmaydi. Yaratilgan maxfiy kalit ma’lumotlarni simmetrik shifrlash jarayonida qo‘llaniladi.

Algoritm ikki tomonga tinglashdan himoyalanmagan, ammo o‘zgartirishdan himoyalangan aloqa kanalida umumiy maxfiy kalitni olish imkonini beradi. Qabul qilingan kalit nosimmetrik shifrlash orqali xabar almashish uchun ishlatilishi mumkin.

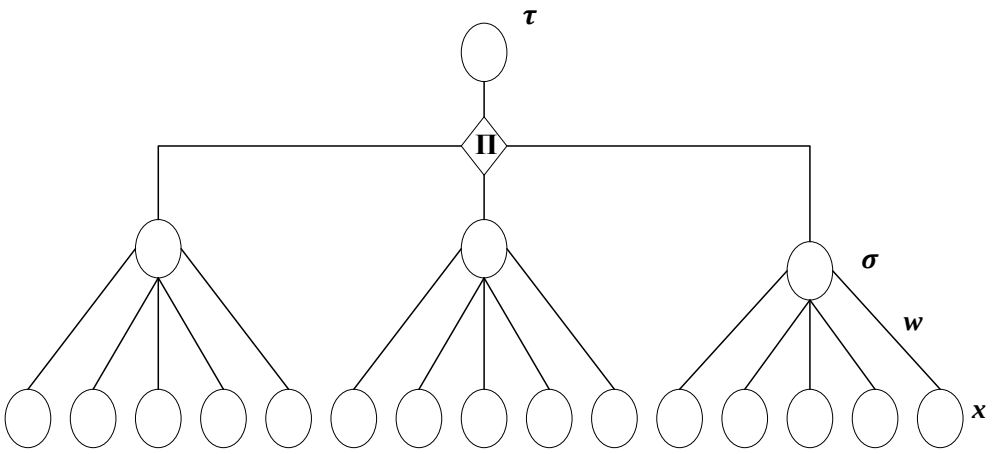
Aytaylik, ikkala abonent ham maxfiy bo‘lmagan va boshqa manfaatdor tomonlarga ham ma’lum bo‘lishi mumkin bo‘lgan ikkita g va p raqamlarini bilishadi. Hech kimga noma’lum bo‘lgan maxfiy kalitni yaratish uchun ikkala abonent ham katta tasodifiy sonlarni hosil qiladi. Birinchi abonent - a sonini , ikkinchi abonent - b sonini. Keyin birinchi abonent $A=g^a mod\ p$ qiymatni hisoblab ikkinchisiga yuboradi, ikkinchisi esa $B=g^b mod\ p$ ni hisoblab birinchisiga yuboradi. Taxminlarga ko‘ra, tajovuzkor ushbu ikkala qiymatni ham olishi mumkin, lekin ularni o‘zgartira olmaydi (uning uzatish jarayoniga aralashish imkoniyati yo‘q). Ikkinchi bosqichda birinchi abonent B tarmog‘i orqali ega bo‘lgan va olgan a soniga asoslanib $B^a mod\ p=g^{ab} mod\ p$ qiymatini hisoblab chiqadi, ikkinchi abonent esa A tarmog‘i orqali ega bo‘lgan va olgan b qiymatiga asoslanib A^bmodp=g^{ab}mod p qiymatini hisoblab chiqadi. Ko‘rib turganingizdek, har ikkala abonent ham bir xil raqamga ega: K=g^{ab} mod p . Bundan ko‘rishimiz mumkinki p, a, b raqamlari yetarlicha katta tanlangan bo‘lsa, ular uni maxfiy kalit sifatida ishlatishlari mumkin. Chunki bu yerda tajovuzkor tutilgan g^amod p va g^bmod p dan g^{ab}mod p ni hisoblashning amalda hal qilib bo‘lmaydigan (oqilona vaqt ichida) muammosiga duch keladi[4].

Diffie-Hellman algoritmining kriptografik barqarorligi (ma’lum p, g A=g^amod p va B=g^bmodp tomonidan K=g^{ab}mod p hisoblash qiyinligi) diskret logarifm muammosining murakkabligiga asoslanadi.

Maxfiy kalitlarni havfsiz almashishni yanada barqarorlashtirish uchun Diffie-Hellman algoritmini sun’iy neyron tarmog‘i bilan alishtirish muammoga yechim bo‘lishi mumkin. Neyron tarmoq kalit almashish usuli va protokoli jihatidan Diffie-Hellman algoritmidan farq qiladi. Buni maxfiy kalitni yaratish uchun neyron tarmog‘ining sinaptik og‘irligi bilan sinxronlashadigan Tree Parity Machines modelidan foydalangan holda amalga oshirish mumkin. Yashirin kalit, o‘z navbatida, Diffie-Hellman maxfiy kalit almashish protokolini amalga oshirishdan ko‘ra xavfsizroqdir va u maxfiy kalit tarqatish protokolining maxfiyligi, ma’lumotlar

yaxlitligi, ob'ekt autentifikatsiyasi kabi xavfsizlik jihatlariga nisbatan qo'llanilishi mumkin.

Kalitlarni xavfsiz almashtirish protokoli ikkita daraxtlar tengligi mashinasini (TPM, tree parity machines-daraxtlar tengligi mashinalari) sinxronlashtirishga asoslangan. TPM - bu ko'p darajali neyronlar tarmog'idir. 1-rasmda $K \times N$ kirish neyronlaridan, K yashirin neyronlardan va bitta chiqish neyronidan iborat. Kirish neyronlari $(1, -1)$ ikkilik qiymatlarni qabul qiladi.



1-rasm. Daraxtlar tengligi mashinasi

Har bir yashirin neyronning qiymati kirish qiymati va og'irlik koeffitsientining yig'indisiga quyidagi shartlar bilan teng:

$$\sigma_i = sign(\frac{1}{\sqrt{N}} \sum_{j=1}^{N} w_{ij}\, x_{ij})$$

$$\text{Sgn}(x)=\begin{cases} -1\,, x \le 0, \\ 1,\ x > 0, \end{cases}$$

bu erda w_{ij} - og'irlik koeffitsienti; x_{ij} - kirish qiymati.

Og'irlik koeffitsientlari kirish neyronlarining yashirin bo'lganlarga nisbatini aniqlaydi va $-L$ dan L gacha qiymatlarni qabul qiladi.

Chiqish neyronining qiymati τ barcha yashirin neyronlarning ko'paytmasiga teng. Chiqish ham ikkilik:

$$\tau = \prod_{i=1}^{K} \sigma_i$$

Shunday qilib, τ yashirin neyronlar sonining $\sigma = -1$ bo'lganda juft yoki toq ekanligini ko'rsatadi. Hammasi bo'lib, 2^{K-1} bir xil natija beradigan ichki permutatsiyalar mavjud τ[5].

Shunday qilib, τ yashirin neyronlar sonining $\sigma = -1$ bo'lganda juft yoki toq ekanligini ko'rsatadi. Hammasi bo'lib, 2^{K-1} bir xil natija beradigan ichki permutatsiyalar mavjud τ.

TPM sinxronizatsiya jarayonining boshida tomonlar mutlaqo tasodifiy, o‘zaro bog‘liq bo‘lmagan og‘irlik koeffitsientlari w bilan bog‘lanadi. Har bir takrorlash, tasodifiy kirish vektori X hosil bo‘ladi va natijada τ qiymati hisoblanadi. Keyin tomonlar o‘z natijalarini taqqoslashadi. Agar τ^A=τ^B bo‘lsa, unda og‘irliklar faqat τ ga teng bo‘lgan maxfiy σ elementi uchun yangilanadi:

w

F(¿¿i^A(t)-$x_i\sigma^A$),

$$w_i^A(t+1) =¿$$

w

F(¿¿i^B(t)-$x_i\sigma^B$),

$$w_i^B(t+1) =¿$$

Qonuniy tomonlar, xuddi har qanday raqib kabi, boshqa tomonlarning og‘irlik vektorlaridan qaysi biri o‘zgartirilganligini bilmaydi. Raqib faqat ushbu signallarni qabul qilishi mumkin, lekin sheriklarga o‘zining chiqish qismi bilan ta’sir qilmaydi. Bu sinxronlashtirishga imkon beradigan, ammo o‘rganish imkonini bermaydigan asosiy omil.

$F(w)$ funktsiyasi og‘irlik omillari L chegarasidan tashqariga chiqmasligiga ishonch hosil qiladi:

F(w)=$\begin{cases} sgn(w) * L, |w| > L, \\ w. \end{cases}$

Tomonlar qisqa vaqt ichida sinxronlashtiriladi, dushmanga qonuniy tomonlar bilan sinxronizatsiya qilish uchun ko‘proq vaqt kerak bo‘ladi. Garchi raqib har bir qadamda A va B qiymatlarni, X kirish vektorini va τ^A, τ^B ni yaratish qoidalarini bilsada, u aloqa davrida sinxronlashtirishga ulgurmaydi[4].

Sun’iy neyron tarmog‘i ommaviy kanal orqali maxfiy kalit almashinuvi protokolidagi xavfsizlikni sezilarli darajada yaxshilaydi. Neyron tarmog‘i algoritmi va sinxronizatsiyasining murakkabligi Diffie-Hellmanga qaraganda ishonchliroq bo‘lib, buzg‘unchining maxfiy kalit almashish jarayoniga xalaqit berishi ehtimolini kamaytiradi bu esa sun’iy neyron tarmog‘idan Diffie Hellman maxfiy kalit almashinuvi protokoliga alternativ sifatida foydalanish mumkinligini ko‘rsatadi. Sun’iy neyron tarmog‘i kiberhujumlarning oldini olish yoki narxini oshirishi mumkin bo‘lgan kalitni yaratishning xavfsiz usulini taqdim etadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. “Researching Neural Networks and Applying for Secret Key Exchange” Sy Truong, 2021
2. “Security Policy and Key Management: Centrally Manage Encryption Key”. Slideshare.net. 2012- 08-13. Retrieved 2013-08-06.
3. Reinholm, James H. “Simplifying the Complex Process of Auditing a Key Management System for Compliance” Cryptomathic. Retrieved 30 May 2016.
4. “An ancient technology gets a key makeover”. Crain’s New York Business. Crain’s New York. Retrieved 19 May 2015.