Kriptografiyada genetik algoritmlarni ishlab chiqish va ularning qo‘llanilishi

Nurjanov Jo‘robek Shomuratovich
nurjanovjorabek1994@gmail.com
Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti stajyor tadqiqotchi talabasi

Kirish

Kriptografiya ma'lumotlarni xavfsiz uzatish va himoyalash uchun ishlatiladigan asosiy fanlardan biridir. Bugungi kunda xavfsizlikka bo‘lgan talablar o‘sib borishi bilan, yangi va samarali kriptografik algoritmlarni ishlab chiqish muhim ahamiyat kasb etmoqda. Genetik algoritmlar (GA) tabiiy tanlanish va evolyutsiya tamoyillariga asoslanib, murakkab muammolarni optimal yechimini topish uchun keng qo‘llaniladi. Ushbu tezisda genetik algoritmlar va ularning kriptografiyada qo‘llanilishi tahlil qilinadi.

1. Kriptografiya asoslari va unga bo‘lgan ehtiyoj.

- **Kriptografiyaning umumiy tushunchasi**: Kriptografiya ma'lumotlarni shifrlash va ularni ruxsatsiz kirishdan himoya qilish uchun qo'llaniladi. Asosiy usullar: simmetrik va asimmetrik shifrlash algoritmlari (AES, RSA).
- **Xavfsizlik masalalari**: Zamonaviy kriptografiya algoritmlarining kuchsiz tomonlari va ularga hujumlar, jumladan, brutal force va manba kodlarini teskari tahlil qilish usullari.

2. Genetik algoritmlarning nazariy xossalari.

- **Genetik algoritmlar tushunchasi**: Genetik algoritmlar (GA) evolyutsiya tamoyillariga asoslangan algoritmlar bo'lib, ular optimal yechimlarni topishda ishlatiladi. GA tabiiy selektsiya, krossover va mutatsiya kabi jarayonlarni modellaydi.
- **Populyatsiya**: Ehtimollik bilan tanlangan yechimlarning dastlabki to'plami.

- **Fitness funksiyasi**: Har bir individning yechim sifatini baholaydigan funksiya.

$$f(x) = cryptographic\ security(x)$$

bu yerda x- kriptografik kalit yoki algoritmning parametrlari.

- **Crossover operator**: Ikkita "parent" yechimlarini birlashtirish orqali yangi yechimlar hosil qilinadi:

$$C(x_1, x_2) = \alpha x_1 + (1-\alpha) x_2$$

bu yerda x_1 va x_2 - parent yechimlar, α esa krossover koeffitsienti.

- **Mutation operator**: Populyatsiya ichidagi yechimlarning ba'zilarida kichik o'zgarishlar kiritiladi, bu esa yechimlarning xilma-xilligini oshiradi.

3. Kriptografiyada genetik algoritmlarning qo‘llanilishi

- **Symmetric key optimization**: Simmetrik kriptografiya algoritmlarida kalitlar uzunligini optimallashtirish uchun GA ishlatiladi. Fitness funksiyasi yordamida kalitlarning xavfsizligi va samaradorligi baholanadi:

$$f(k) = \max\left(security\_index(k) - brute\_force\_resistance(k)\right)$$

bu yerda k - kalit parametrlari.

- **Optimizing cryptographic algorithms**: Genetik algoritmlar shifrlash algoritmlarining parametrlarini (kalit uzunligi, operatsiyalar soni va algoritmning parametr konfiguratsiyasi) optimallashtiradi.

- **RSA key generation**: Genetik algoritmlar RSA algoritmi uchun katta prime-sonlarni tanlash jarayonida ishlatiladi:

$$f(p,q) = \min(N)\ where\ N = p \cdot q$$

bu yerda p va q yopiq sonlar bo'lib, ulardan RSA kaliti hosil qilinadi.

4. Kriptografik masalalarda genetik algoritmlarning ishlash bosqichlari.

- **Populyatsiyani yaratish**: Boshida ma'lum bir o'zgaruvchi qiymatlar to'plami ishlab chiqiladi. Misol uchun, simmetrik kalitlar ketma-ketligi populyatsiya sifatida yaratiladi.

- **Fitness funksiyasini hisoblash**: Har bir kalit yoki shifrlash jarayonining xavfsizlik darajasini aniqlash uchun fitness funksiya ishlatiladi.

- **Krossover va mutatsiya**: Krossover operatori orqali kalitlar yoki algoritm parametrlarining eng optimal kombinatsiyalari yaratiladi. Mutatsiya operatori esa yangi innovatsion yechimlarni kiritadi.
- **Tanlanish va keyingi avlod**: Eng samarali yechimlar tanlanib, yangi avlodga o'tkaziladi.

Xulosa

Kriptografiyada genetik algoritmlarni qo‘llash ma'lumotlarni himoya qilishning yangi va samarali usuli hisoblanadi. Genetik algoritmlar orqali kriptografik tizimlarning xavfsizlik parametrlarini optimallashtirish va zamonaviy xavf-xatarlarga qarshi samarali yechimlarni ishlab chiqish mumkin. Kelajakda genetik algoritmlar va boshqa ilg‘or texnologiyalarni birlashtirish orqali yanada kuchli va bardoshli kriptografik tizimlar yaratish kutilmoqda.

Foydalanilgan adabiyotlar

1. **Bagane, P., & Sirbi, D. K.** (2021). *Comparison between traditional cryptographic methods and genetic algorithm based method towards Cyber Security*. International Journal of Advanced Research.
2. **Jhingran, R., Thada, V., & Dhaka, S.** (2015). *A study on cryptography using genetic algorithm*. International Journal of Computer Science.
3. **Turčaník, M., & Javurek, M.** (2019). *Cryptographic Key Generation by Genetic Algorithms*. Information & Security.
4. **Sen, A., Ghosh, A., & Nath, A.** (2017). *Bit level symmetric key cryptography using genetic algorithm*. 7th International Conference on Computer and Communication Technologies.