

KRIPTOTAHLILDA TABIIY ALGORITMLAR

Berdimurodov Mansur Alisherovich

O'zbekiston xalqaro islom akademiyasi

katta o'qituvchisi PhD.

e-mail: mansur_alisherovich@mail.ru

Ramazonov Shamsiddin Shovkat o'g'li

O'zbekiston Milliy universiteti o'qituvchisi

e-mail: ramazonov377@gmail.com

Dusmurodov Qodir Albert o'g'li

Toshkent axborot texnologiyalari universiteti magistri

e-mail: Dqodir3366@mai.ru

***Annotatsiya.** Ushbu ishda tabiiy algoritmning kriptotaliz masalasida tatqiqi asosida maqsad funksiya aniqlandi. Hamda aniqlangan maqsad funksiya asosida genetik algoritm kriptotalizda qo'llanish algoritmi taklif qilindi. Taklif qilingan algoritm asosida dasturiy mahsulot yaratilgan bo'lib dasturiy mahsulot haqida ma'lumot keltirib o'tilgan. Shuningdek, ishda tabiiy algoritmlar chumoli va asalari algoritmlari haqida ma'lumotlar keltirib o'tilgan. Kriptotalhilda genetik algoritmni qo'llash uchun maqsad funksiyani tanlash shartlari va ingliz tilidagi to'liq aniqlanmagan matnni ingliz tilidagi bigrammalar va tabiiy algoritm dan foydalangan holda to'liq matnni tiklash algoritmi, xromosomalarning harakatini tanlash usullari algoritmlari va standart genetik algoritm sxemasi keltirib o'tilgan.*

***Kalit so'zlar:** Kriptotalhil, tabiiy algoritm, genetik algoritm, chastatasi, bigramma, maqsad funksiya, xromosoma, asalari algoritmi.*

ЕСТЕСТВЕННЫЕ АЛГОРИТМЫ В КРИПТОАНАЛИЗЕ

Бердимурадов Мансур Алишерович

Международная исламская академия Узбекистана

старший преподаватель к.ф.н.

Рамазонов Шамсиддин Шовкат угли

Преподаватель Национального университета Узбекистана

Дусмуродов Кодир Альберт угли

Магистр Ташкентского университета информационных технологий

Аннотация. В данной работе определена целевая функция на основе исследования естественного алгоритма в задаче криптоанализа. На основе выявленной целевой функции предложен генетический алгоритм для использования в криптоанализе. На основе предложенного алгоритма создан программный продукт, даны сведения о программном продукте. Также в работе даны сведения о естественных алгоритмах — муравьином и пчелином алгоритмах. Приведены условия выбора целевой функции для применения генетического алгоритма в криптоанализе и алгоритма полнотекстового восстановления с использованием английских биграмм и естественного алгоритма, алгоритмы выбора методов перемещения хромосом, схема стандартного генетического алгоритма.

Ключевые слова: криптоанализ, естественный алгоритм, генетический алгоритм, частота, биграмма, целевая функция, хромосома, пчелиный алгоритм.

NATURAL ALGORITHMS IN CRYPTOANALYSIS

Berdimuradov Mansur Alisherovich

International Islamic Academy of Uzbekistan

senior teacher PhD.

Ramazonov Shamsiddin Shovkat ugli

Teacher of the National University of Uzbekistan

Dusmurodov Qodir Albert ugli

Master of Tashkent University of Information Technologies

Abstract. In this work, the objective function was determined based on the research of the natural algorithm in the problem of cryptanalysis. Based on the identified objective function, the genetic algorithm was proposed for use in cryptanalysis. A software product was created based on the proposed algorithm, and information about the software product was given. Also, information about

natural algorithms, ant and bee algorithms, is given in the work. The conditions for the selection of the objective function for the application of the genetic algorithm in cryptanalysis and the full-text recovery algorithm using the English bigrams and the natural algorithm, the algorithms of the selection methods of the movement of chromosomes, and the scheme of the standard genetic algorithm are presented.

Key words: *Cryptanalysis, natural algorithm, genetic algorithm, frequency, bigram, objective function, chromosome, bee algorithm.*

Kirish

Rivojlanayotgan tadqiqot yoʻnalishi sifatida toʻda razvedkasi 1980-yillarda kontseptsiya taklif qilinganidan beri koʻplab tadqiqotchilarning eʼtiborini tortdi. Hozirgi vaqtda u fanlararo chegaraga aylandi va koʻplab fanlar, jumladan sunʼiy intellekt, iqtisod, sotsiologiya, biologiya va boshqalarning diqqat markazi hisoblanadi. Baʼzi turlar shafqatsiz tabiatda odamlarning donoligidan koʻra, toʻdalarning kuchidan foydalangan holda omon qolishlari uzoq vaqtdan beri kuzatilgan. Bunday toʻdadagi shaxslar unchalik aqlli emas, lekin ular hamkorlik va mehnat taqsimoti orqali murakkab vazifalarni bajaradilar va murakkab masalalarni ham yecha olmoqdalar va oʻz-oʻziga moslasha oladigan butun toʻda sifatida yuqori aql-zakovatni namoyon etmoqdalar. Toʻda (Swarm) razvedkasi yoki tabiiy algoritmlar deb yuritiladigan bir nechta algoritmlar bor jumladan chumoli algoritmi, asalari algoritmi va hokozo[4,5,6].

Toʻda yuqori mustahkamlik va moslashuvchanlikka ega boʻlgan holda murakkab shaxs qila oladigan vazifalarni bajarishi mumkin. Toʻda razvedkasi markazlashtirilgan boshqaruv va global modelga muhtoj boʻlmasdan toʻdaning toʻliq afzalliklaridan foydalanadi va keng koʻlamli murakkab muammolar uchun ajoyib yechimni taʼminlaydi[8].

Adabiyotlar tahlili

1989-yilda Gerardo Beni va Vang Jing “Sharm intelligence” (RI) atamasini kiritdilar. (ingliz. Swarm Intelligence, SI). Bu atama uyali robotlar tizimi uchun ishlatilgan va markazlashmagan oʻzini oʻzi tashkil qilish tizimining kollektiv xatti-

harakatlarini nazarda tutgan. Bundan tashqari hozirda qator Саймон Д., Л.А.Гладков, В.В.Курейчик, В.М.Курейчик, Ю.А.Скобцов kabi olimlar genetik algoritmlarni har xil sohada optimallashtirish usullari sifatida qarab o'tganlar. Genetika algoritmlari sohasidagi tadqiqotlar asosan nazariy bo'lib, ular 80-yillarning o'rtalariga qadar Pittsburg Pensilvaniya shtatida (AQSh) genetika algoritmlari bo'yicha birinchi xalqaro konferentsiya o'tkazilgunga qadar saqlanib qoldi[8].

Mashinali o'rgatishda evolyutsion tamoyillarni qo'llash g'oyasi A. Turingning "O'ylaydigan" mashinalarni yaratish muammolariga bag'ishlangan ilmiy ishlarida ham qaralgan [7].

Tadqiqot metodologiyasi

Asalari algoritmi haqida. Asalarilar koloniyasi algoritmi (sun'iy asalarilar koloniyasini optimallashtirish) kompyuter fanlari va operatsiyalarni tadqiq qilishda optimallashtirish masalalarini hal qilish uchun polinomli evristik algoritmlardan biridir. Tabiatda nektar yig'ishda asalarilar koloniyasining xatti-harakatlariga taqlid qilishga asoslangan stoxastik bionik algoritmlar toifasiga kiradi. Algoritmlarning asosi nektar izlashda asalarilarning xatti-harakatlarini matematik modellashtirishdir. Ikki darajali qidiruv strategiyasi algoritmning asosiy g'oyasini o'z ichiga oladi. Skaut asalarilardan foydalanish orqali, istiqbolli pozitsiyalarning tasodifiy to'plami (nektar manbalari). Uyaga qaytib kelganda, asalarilar topilgan manbagacha bo'lgan masofa haqidagi kodlangan ma'lumot uzatiladigan "chayqalish raqsi" (aslida, asalarilar o'rtasidagi aloqaning o'ziga xos shakli) ni amalga oshiradilar. Oziq-ovqat, bu manbaga yo'nalish haqida, u yerda topilgan nektarning sifati va miqdori haqida.

Asalari koloniyasi algoritmi komponentalari. Model 4 ta komponentadan iborat:

1. Oziq-ovqat manbalari hal qilinayotgan muammoning yechimlarini ifodalaydi. Har bir oziq-ovqat manbai muammoni hal qilishning mosligiga mutanosib ravishda nektar ishlab chiqaradi.

2. Ish bilan ta'minlangan asalarilar avvalgi oziq-ovqat manbalariga qaraganda ko'proq nektarga ega bo'lgan yangi oziq-ovqat manbalarini qidirishadi. Ushbu qidiruv tasodifiy, ammo boshqa oziq-ovqat manbalaridan ma'lum ma'lumotlardan foydalanadi.

3. Tomoshabin asalarilar ishlaydigan asalarilarning chayqalish raqsini tomosha qiladilar va oziq-ovqat manbalarini o'rganadilar. Amalda, bu Ruletka g'ildiragini tanlash algoritmi yordamida erishiladi, bu esa katta ehtimollik bilan yuqori nektarga ega bo'lgan oziq-ovqat joylarini tanlashga olib keladi.

4. Skaut asalarilar tashlab ketilgan oziq-ovqat manbalarini almashtirish uchun o'zlarining oziq-ovqat manbalarini tasodifiy tanlaydilar, ularni oldindan belgilangan miqdordagi yo'llar orqali yaxshilash mumkin emas.

Asalari koloniyasi algoritmi qo'llanilishi. Pythonda algoritmni amalga oshirish: Pybee moduli quyidagi sinflarni o'z ichiga oladi: **floatbee** – suzuvchi nuqta raqamlari bilan tasvirlangan asalarilar uchun asosiy sinf. **Xiva** – eng yaxshi va tanlangan maydonlarni tanlash uchun algoritmning asosiy harakatlari, shuningdek, asalarilarni kerakli lavozimlarga jo'natish uchun uyaning klassi.

Asalari koloniyasi algoritmi qo'llanilishi

- *runcount*-bu mustaqil algoritmni ishga tushirish soni. Algoritm asosan tasodifiy miqdorlarga bog'liq bo'lgani uchun, bir nechta ishga tushirish, shuningdek, barcha boshlang'ichlarning o'rtacha miqdori algoritmning o'xshashligini faqat bir marta ishga tushirishdan ko'ra aniqroq ko'rsatadi. Bu holda, standart algoritm faqat bir marta boshlanadi.
- *maxiteration*-algoritmning eng ko'p sonli iteratsiyasi. Bunday holda, bu to'xtatishning yagona mezonidir. Bu bir nechta ishga tushirish bo'yicha ish natijalarini o'rtacha hisoblash osonroq bo'lishi uchun amalga oshiriladi. Agar boshqa to'xtatish mezonlari joriy etilsa, unda har bir boshlang'ich uchun statistikani to'plash uchun sinfda natijalar bilan ro'yxatlar turli uzunliklarda bo'ladi.
- *max_func_counter* eng yaxshi yechimni bermaydigan qancha yinelemalarni aniqlaydi, yechimlarni topish uchun maydonlarning o'lchami kamayadi.

Ya'ni, bu holda, agar 10 elementlardan, avvalgidan ko'ra yaxshiroq yechim topilmasa, hive ro'yxati tomonidan berilgan maydon oralig'i, statik usuli *getrangecoeff()* sinf asalarilar tomonidan qaytarib ro'yxatiga ko'ra kamayadi, ya'ni, bu holda hajmi 0.98 tomonidan ko'paytiriladi bo'ladi.

Genetik algoritmlar o'z-o'zini tartibga soluvchi xatti-harakatlarga ega bo'lgan ko'p agentli aqlli optimallashtirish tizimi. Swarm algoritmlari (RA) suruvdagi qushlar yoki baliqlarning yoki to'dadagi hasharotlarning ijtimoiy xatti-harakatlarini modellashtirishga asoslangan. Algoritmlar murakkab kompleks optimallashtirish masalalarini hal qilishda qo'llanilishini topadi. Yechish mumkin bo'lgan yechimlarning diskret to'plamidan maqsad funksiyasining minimal yoki maksimalini topishdan iborat.

Tahlillar va natijalar

Kriptotahlilda genetik algoritim. Yuqoridagi ma'lum bo'ldiki Tabiiy algoritmlar odatda maksimalni yoki minimalni topish. Maqsad funksiyani tanlab olishga qarab optimallashtirish masalalarini yechish uchun ishlatiladi. Kriptoanaliz masalalarida tabiiy algoritmlarni tatqiq qilishda to'la ochilmagan kalit yoki matnlarni analiz qilishda to'liq ochishda foydalanish mumkin. Bunda fitness funksiyani shifr matn yoki kalit qaysi tilda yozilgani muxim parametr hisoblanadi. Chunki har bir tilda harflar va n -grammlarning qiymati har xil bo'ladi.

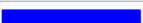
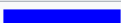
Bigramma yoki diagramma – bu odatda harflar, bo'g'inlar yoki so'zlardan iborat bo'lgan belgilar qatoridan ikkita qo'shni elementlarning ketma-ketligi. Bigramma $n = 2$ uchun n -grammdir.

Biz ingliz tilidagi to'liq ochilmagan matnni ingliz tilidagi bigrammalar va tabiiy algoritmdan foydalangan holda to'liq matnni tiklash algoritmini taklif qildik. Dissertatsiya ishida taklif qilingan algoritim to'liq qidirishdan kura ancha samarali ekanligini oddiy matematik hisob kitoblar yordamida hisoblash ko'rsatish mumkin. $M = \text{"_he text is g_ven _n _ngli_h"}$ kabi chala aniqlangan matn berilgan bo'lsa bu matnda beshta noma'lum harf bor va bo'lishi mumkin bo'lgan matnlar soni 26^5 ni tashkil etadi. Genetik algoritim bilan esa samarali aniqlash mumkin.

Quyida ingliz tilidagi harflarning chastotasi keltirib o‘tilgan(1-rasm). Harflar kabi bigrammalar ham aniqlanadi.

Ingliz tilida foizi ko‘p bo‘lgan Bigrammalar chastotasi quyidagicha

th 3.56%	nd 1.35%	al 1.09%	ou 0.87%	ro 0.73%
he 3.07%	ti 1.34%	ar 1.07%	io 0.83%	ic 0.70%
in 2.43%	es 1.34%	st 1.05%	le 0.83%	ne 0.69%
er 2.05%	or 1.28%	to 1.05%	ve 0.83%	ea 0.69%
an 1.99%	te 1.20%	nt 1.04%	co 0.79%	ra 0.69%
re 1.85%	of 1.17%	ng 0.95%	me 0.79%	ce 0.65%
on 1.76%	ed 1.17%	se 0.93%	de 0.76%	
at 1.49%	is 1.13%	ha 0.93%	hi 0.76%	
en 1.45%	it 1.12%	as 0.87%	ri 0.73%	

E	13%		11%	
T	9.1%		6.7%	
A	8.2%		7.8%	
O	7.5%		6.1%	
I	7%		8.6%	
N	6.7%		7.2%	
S	6.3%		8.7%	
H	6.1%		2.3%	
R	6%		7.3%	
D	4.3%		3.8%	
L	4%		5.3%	
C	2.8%		4%	
U	2.8%		3.3%	
M	2.4%		2.7%	
W	2.4%		0.91%	
F	2.2%		1.4%	
G	2%		3%	
Y	2%		1.6%	
P	1.9%		2.8%	
B	1.5%		2%	
V	0.98%		1%	
K	0.77%		0.97%	
J	0.15%		0.21%	
X	0.15%		0.27%	
Q	0.095%		0.19%	
Z	0.074%		0.44%	

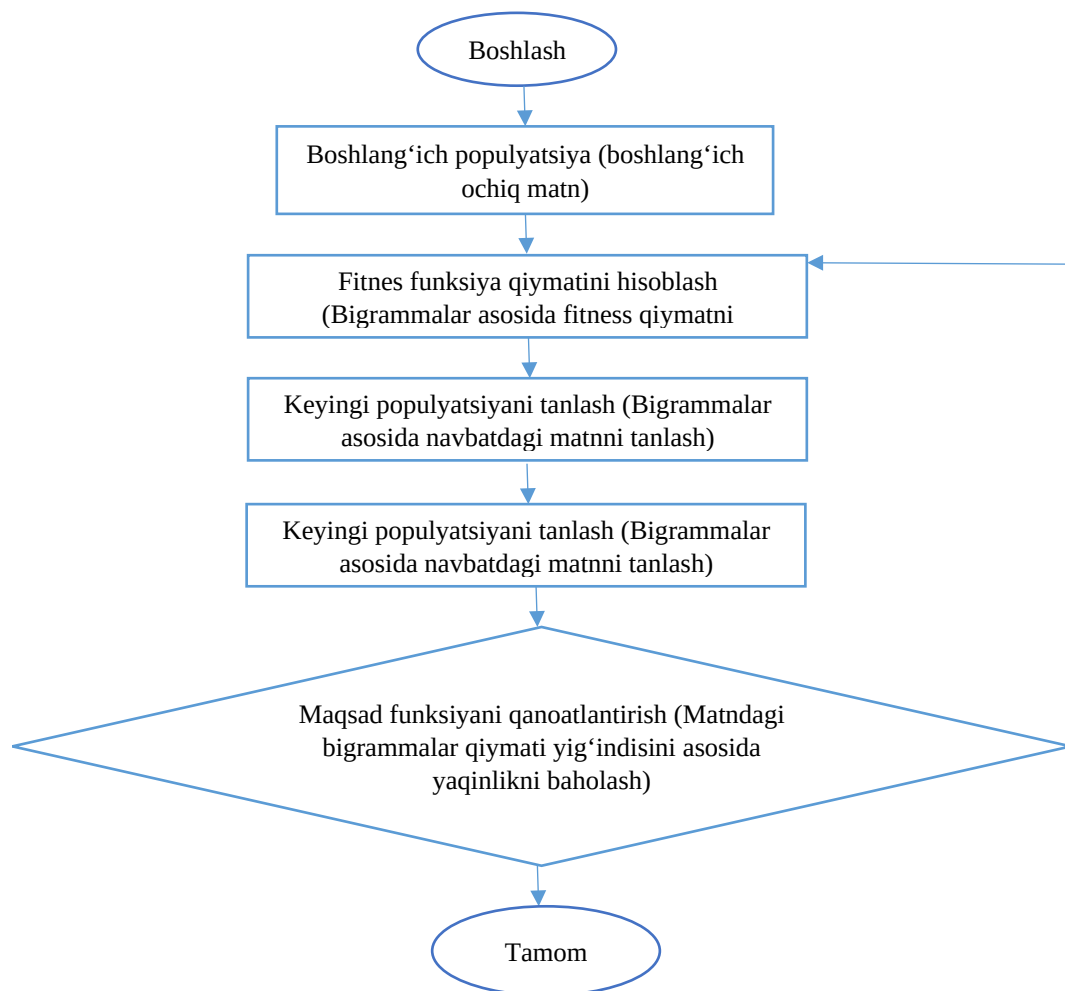
1-rasm. Ingliz tilida harflar chastotasi

Sintaktik n -grammalar matnning chiziqli tuzilishidan ko‘ra sintaktik bog‘liqlik yoki tarkibiy daraxtlardagi yo‘llar bilan belgilanadigan n -grammalardan ham foydalanish mumkin. Masalan, “iqtisodiy yangiliklar moliya bozorlariga unchalik ta’sir qilmaydi” jumlasini bog‘liqlik munosabatlarining daraxt

tuzilmasidan so'ng sintaktik n -grammalarga aylantirish mumkin: Bunda yangiliklar-iqtisodiy, ta'sir qilmaydi, ta'sir, moliyaviy bozor kabi n grammalar aniqlanadi[1,2,3].

Sintaktik n -grammalar chiziqli n -grammalarga qaraganda sintaktik tuzilmani aniqroq aks ettirish uchun mo'ljallangan vektor fazo modelidagi xususiyatlar yo'liga ega,. Muayyan vazifalar uchun sintaktik n -gramlar, masalan, mualliflik atributi uchun standart n -gramlardan foydalanishga qaraganda yaxshiroq natijalar beradi.

Sintaktik n -grammalarining yana bir turi - matnning nutq qismi ketma-ketliklaridan ajratib olinadigan qat'iy uzunlikdagi qo'shni bir-biriga o'xshash ketma-ketliklar sifatida belgilanadigan nutq qismi n -gramlari[4,7].



2-rasm. Standart genetik algoritim (GA) sxemasi

Kriptoanalizda tabiiy algoritmlarining tadqiq qilish dasturiy taminoti va algoritmi

Kriptoanalizda maqsad funksiyasi. Kriptoanalizda tabiiy algoritmlardan foydalanishda maqsad funksiyani va xromasomani ehtimoliy yo'lini tanlash algoritmi aniqlash muxim hisoblanadi. Biz ushbu dissertatsiya ishida to'liq aniqlanmagan matndagi noma'lum belgilarini aniqlashda genetic algoritmdan foydalanishda harflar va bigrammalardan foydalanish asosida maqsad funksiyani belgilab oldik. Taklif etilgan algoritm quyidagi qadamlardan iborat.

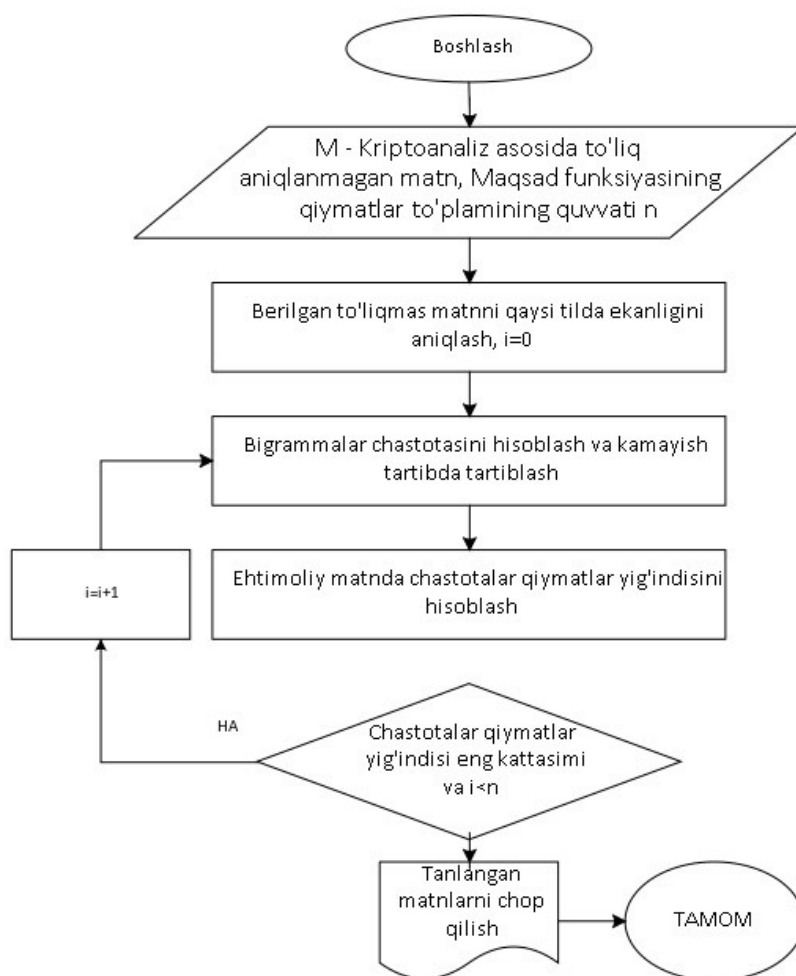
- 1) To'liq aniqlanmagan matnning qaysi tilda yozilganligini aniqlash.
- 2) Matn qaysi tildaligi aniqlangandan so'ng, usha tilda harflar va bigrammalarni chastotasi hisoblash. Buning uchun usha tilda yozilgan katta matn kerak bo'ladi.
- 3) Bigrammaning chastotasi katta qiymatidan boshlab tekshirib ko'riladi. Butun matn bo'yicha bigrammalar chastotalar qiymatlarining yig'indisi hisoblanadi.
- 4) Butun matn bo'yicha bigrammalar chastotasining qiymatlari yig'indisi kamayish tartibida aniqlanadi.
- 5) Oldindan berilgan maqsad funksiyasi bilan aniqlangan to'plamning quvvaticha mumkin bo'lgan matnlarni ekranga chiqarish.
- 6) Aniqlangan mumkin bo'lgan matnlar ichidan tanlab olinadi.

Alifboda belgilar soni a ta bo'lgan matn uzunligi n bo'lsa, noma'lum belgilar soni m ta bo'lsa, mumkin bo'lgan jami holatlar soni a^m ta bo'ladi. Bigrammalarning chastotaviy qiymatlar yig'indisi maksimal $2m$ bo'lishi mumkin.

Misol uchun to'liq aniqlanmagan matn $M = \text{" t_e book t_xt"}$ maqsad funksiyasining qiymatlar to'plami quvvati 4ga teng bo'lsin. Mos ravishda bo'lishi mumkin bo'lgan matnlar quyidagi kabi aniqlandi.

- 1) the book text
- 2) tre book tixt
- 3) tte book taxt
- 4) tse book toxt

Aniqlangan matnlardan tekshirib 1) ekanligini aniqlash mumkin.



3-rasm. Genetik algoritmi asosida taklif qilingan algoritmi blok sxemasi

Kriptoanalizda tabiiy algoritmlarining dasturiy taminoti

Ushbu maqolada keltirilgan maqsad funksiya asosida bajarilgan dasturiy mahsulot C# dasturlash tili, Visual Studio 2019 muhitida yaratilgan. Dastur asosiy oynasida matnni kiritish uchun oyna, chastonani, bigrammalarni hisoblash, fayldan o'qish, dasturni yopish va Genetik algoritmi to'liq ochilmagan matnni tahlil qilish uchun G_A kabi tugmalari bor. Shuningdek chastotani hisoblash tugmasi kiritilgan matndagi belgilarni chastotasini kamayish tartibida, ASCE kodini va belgini o'zini shuningdek matnda bu belgi qancha foizni tashkil etishini hisob ekranga chiqaradi. Bu bizga maqsad funksiyani hisoblashda asosiy qiymat bo'lib xizmat qiladi. Shuningdek dasturda bigrammani hisoblash tugmasi esa matndagi bigrammalarni hisoblaydi. G_A tugmasi bosilganda yangi oyna ochiladi hamda bu oynada alohida amallar bajariladi (4-rasm).

Form1

Mirzo Ulug'bek nomidagi o'zbekiston Milliy universiteti

G_A	Chastatani hisoblash	Bigrammani hisoblash	Fayldan o'qish	Dasturni yopish
		1. 105 i 9 16,36		
		2. 32 5 9,09		
		3. 101 e 4 7,27		
		4. 111 o 4 7,27		
		5. 110 n 3 5,45		
		6. 108 l 3 5,45		
		7. 116 t 3 5,45		
		8. 107 k 2 3,64		
		9. 98 b 2 3,64		
		10. 39 ' 2 3,64		
		11. 103 g 2 3,64		
		12. 114 r 2 3,64		
		13. 115 s 2 3,64		
		14. 77 M 2 3,64		
		15. 117 u 2 3,64		
		16. 122 z 2 3,64		
		17. 109 m 1 1,82		
		18. 100 d 1 1,82		
		19. 97 a 1 1,82		
		20. 118 v 1 1,82		
		21. 121 y 1 1,82		

4-rasm. Kritilgan matnda chastota va bigrammani hisoblash

Yangi genetik algoritm asosida to'liqmas matnni tiklash oynasida sodda shifrlash algoritmlari Sezar, Vijiner va Vernam algoritmlari bilan shifrlash va deshifrlash imkoniyati ham mavjud. Shuningdek maqsad funksiyasining qiymatlar to'plamining quvvati ham kiritish mumkin.

M=

Kalit:

Shifr:

Taxminiy ochiq matn:

Mumkin bo'lgan ochiq matnlar:

Yaqinlik qiymati:

5-rasm. Sezar shifrlash va deshifrlash oynasi

To'liq aniqlanmagan matn tahlilida genetik algoritmi qo'llagan holda mumkin bo'lgan matnlarni qurish algoritmi asosida yaratilgan dasturiy mahsulotning chastotaviy kriptotalizdan yaxshi tomoni chastotaviy tahlilda shifr

Taxminiy ochiq matn:

MATNni aniqlash **Yopish**

Mumkin bo'lgan ochiq matnlar:

Yaqqinlik qiymati:

the text books
tre tixt books
tte taxt books
tse toxt books

matn katta

6-rasm. To'liqmas matndan genetik algoritmi asosida mumkin bo'lgan matnlarni aniqlash

bo'lsa aniqlik oshadi va kichkina matnlarga samarasi kam hisoblanadi. Biz taklif qilgan genetik algoritmda esa shifr qaysi tilda ekanligi aniq bo'lsa, to'liq ochilmagan matnni ehtimoli yuqori ya'ni maqsad funksiyaga eng yaqinidan boshqa qarab o'tishimiz mumkin bo'ladi. 6-rasmda mumkin bo'lgan matnlarni aniqlash dasturining ishlash oynasi keltirilgani.

Xulosa

Ushbu maqolada tabiiy algoritmi kriptotalil masalasida tatbiq qilish qarab o'tildi. Genetik algoritmlarning asosi bo'lgan maqsad funksiya Kriptotalil masalasi uchun aniqlandi. Hamda aniqlangan maqsad funksiya asosida genetik algoritmi kriptotalizda qo'llab dasturi yaratildi. Dasturiy mahsulot asosida ingliz tilidagi to'liq ochilmagan matn tahlil qilib misollar ham keltirib o'tildi. Bu dasturiy mahsulot haqida ma'lumot keltirib o'tildi.

Shuningdek maqolada tabiiy algoritmlar chumoli va asalari algoritmlari haqida ma'lumotlar keltirib o'tilgan. Kriptotalilda genetik algoritmi qo'llash uchun maqsad funksiyani tanlash shartlari va ingliz tilidagi to'liq ochilmagan matnni ingliz tilidagi bigrammalar va tabiiy algoritmdan foydalangan holda to'liq

matnni tiklash algoritmi, xromosomalarning harakatini tanlash usullari algoritmlari va standart genetik algoritm sxemasi qurildi.

Foydalanilgan adabiyotlar.

1. Akbarov D.Y. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi // Toshkent, 2008, -B. - 394.
2. Jo'rayev G'.U.Kriptotahlil elementlari fanidan ma'ruzalar matni // Toshkent, 2021, -B. - 64.
3. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. Kriptotahlil va uning maxsus usullari – Toshkent, 2010 – 175 bet.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.М.: ТРИУМФ. 2003.
5. Саймон Д. Алгоритмы эволюционной оптимизации. — М.: ДМК Пресс, 2020. — 940 с. — [ISBN 978-5-97060-812-8](#).
6. Гладков Л. А., Курейчик В. В., Курейчик В. М. Генетические алгоритмы: Учебное пособие. — 2-е изд. — М.: Физматлит, 2006. — 320 с. — [ISBN 5-9221-0510-8](#).
7. Скобцов Ю. А. Основы эволюционных вычислений. — Донецк: ДонНТУ, 2008. — 326 с. — [ISBN 978-966-377-056-6](#).
8. www.wikipedia.org