KRIPTOGRAFIYADA FRAKTALLARDAN FOYDALANISH IMKONIYATLARI

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

Annotatsiya. Maqola fraktal kriptografiyasi masalalarini hal qilish uchun ishlab chiqilgan algoritmni ko‘rib chiqishga bag‘ishlangan, xususan, Mandelbrot va Julia fraktal ketma-ketliklariga asoslangan asimmetrik algoritm keltirib o’tilgan.

Kalit so‘zlar: fraktal kriptografiya, xesh-funksiya, algoritm, iteratsiyalar, murakkab sonlar.

Fraktal kriptografiya - bu ilg‘or, ishonchli va xavfsiz xabarlar uzatish tizimlarini yaratish uchun mo‘ljallangan tizimdir, bu esa ikki va uch o‘lchamli fraktal fazolar yordamida amalga oshiriladi. Ushbu yo‘nalish yangi hisoblanadi. Fraktal kalitlarni uzatish texnologiyasi hali rivojlanishning dastlabki bosqichida. Hozirgi vaqtda u XX asrning standart tushunchalarini shifrlar va kodlar uchun qo‘llaydi.

Fraktallarning xaosli xatti-harakati ma’lumotlarni shifrlash uchun ishlatilishi mumkin. Fraktal kriptografiyada kalitlar yo‘q, iteratsiyalar ishlatiladi. Xavfsizlik rekursiv funksiyaning oldindan aytib bo‘lmaydiganligiga asoslangan (n-iteratsiyani hisoblash uchun avval n-1 iteratsiyani hisoblash kerak). Oddiy kriptografiyada bo‘lgani kabi, qancha ko‘p iteratsiyadan foydalanilsa, shuncha yaxshi, chunki ko‘p marta iteratsiyadan o‘tgan fraktal nuqtasi boshidan ancha uzoqlashadi va nuqtaning yo‘lini har bir algoritm qadamini bajarib bo‘lmay turib hisoblab bo‘lmaydi.

Ko‘rib chiqilgan ishlarda shifrlovchi algoritmlarda fraktallardan foydalanish quyidagilar uchun taklif etiladi:

- algoritmning mustahkamligini kalitni cheklanmagan uzunlikda yaratish imkoniyati orqali oshirish;
- psevdotasodifiy ketma-ketliklar yaratish;
- almashtirish shifrlari va o‘rnini bosuvchi shifrlar amalga oshirish;
- turli xil tasvirlarning vizual kriptografiyasini amalga oshirish.

Fraktallardan foydalanish asosidagi simmetrik shifrlash prinsiplari [1]da ko‘rib chiqilgan.

Asosiy g‘oya quyidagicha, avvalo, gamma funksiyasi yordamida gamma ketma-ketlik ishlab chiqariladi, bu ketma-ketlik K parametriga bog‘liq bo‘lib, u iteratsion funksiyaning boshlang‘ich qiymatlarini belgilaydi. Shundan so‘ng, asosiy signal

olingan gamma bilan 2 moduli bo‘yicha bitma-bit qo‘shiladi. Natijada shifrlangan ma’lumotlar olinadi.

Deshifrovka ham ma’lumotlar va K parametri yordamida olingan gamma qo‘shilishi orqali 2 moduli bo‘yicha amalga oshiriladi. Iteratsion funksiyani boshlang‘ich parametrlari, bu algoritm uchun mumkin bo‘lgan bir qator o‘zgarishlardan birini tanlashni ta’minlaydi, kriptografik kalit hisoblanadi.

Boshqa turdagi simmetrik shifrlash, algebraik fraktallardan bir marta ishlatiladigan bloknot yaratish uchun ishlatiladi, bu [2] va [3] ishlarida ko‘rib chiqilgan.

Fraktallardan foydalanish asosidagi asimmetrik shifrlash prinsiplari [4], [5], [6] tadqiqotlarida ko‘rib chiqilgan.

Fraktal shifrlash usullari o‘zining kuchli va zaif tomonlariga ega. Materiallarni o‘rganish davomida fraktallardan shifrlashda foydalanishning kuchli va zaif tomonlarini ajratib ko‘rsatishimiz mumkin.

Kuchli tomonlarga quyidagilar kiradi:

- fraktal ketma-ketlik yordamida sifatli tasodifiy sonlar generatorlarini olish mumkin;

- fraktal ketma-ketliklar bir tomonlama funksiyalarni o‘z ichiga oladi (iteratsion funksiyaning oldingi qiymatini aniq hisoblab bo‘lmaydi);

- amalga oshirishning oddiyligi, fraktal ketma-ketligining keyingi qiymatini hisoblash uchun faqat bitta funksiya kifoya;

- kalitning hajmini o‘zgartirmasdan algoritmni o‘zgartirish imkoniyati mavjud (yangi turdagi murakkab sonni yaratish yoki o‘zgartirish va ularga matematik amallarni aniqlash talab qilinadi).

Zaif tomonlarga quyidagilar kiradi:

- algoritmlar yetarlicha o‘rganilmagan (bu yo‘nalish kriptografiyada yangi hisoblanadi);

- algoritmlar standartlashtirilmagan (amaliy qo‘llanilishi, hujjatlari yoki standartlari yo‘q);

- algoritmlar keng tarqalmagan;

- apparatda amalga oshirilmagan (fraktal shifrlashdan foydalanadigan kriptografik protsessor yo‘q);

- fraktallar simmetriya xususiyatiga ega, bu kalitni tanlash maydonini qisqartiradi; kuchsiz va kuchli kalitlarning mavjudligi;

- o‘zgaruvchan nuqtali amallarni bajarish (bu amallar taxminan va butun sonlar bilan amallarga qaraganda ancha uzoq vaqt davomida bajariladi);

- murakkab sonning binar yozuvda 0 va 1 ning iteratsiyadan iteratsiyaga notekis o‘zgarishi;

- o‘zgaruvchan nuqtali sonni 0 va 1 ning teng tarqalgan binar ketma-ketligiga aylantirish uchun qo‘shimcha amallar zarurati;

- parallel hisob-kitoblarni tashkil qilish qiyinligi;

- kalitni uzatish standarti yo‘q.

Taklif etilgan algoritm fraktal shifrlash algoritmlari orasida yangi bo‘lib, shuningdek umuman shifrlash algoritmlari orasida yangidir.

2007 yilda [6]-da Mandelbrot va Julia to‘plamlariga asoslangan kalitlar almashinuv protokoli taklif etilgan va Diffi-Hellman protokoli bilan taqqoslovchi tadqiqot keltirilgan. Fraktal tushunchasidan foydalanuvchi ochiq kalitli shifrlash kriptografik protokoli tavsiflangan, bu yondashuv an'anaviy sonlar nazariyasiga asoslangan ochiq kalitli shifrlash protokoliga nisbatan ancha ustunligini ko‘ rish mumkin. Shuningdek, katta butun sonlarni omillarga ajratish masalasining hisoblash murakkabligiga asoslangan RSA ochiq kalitli kriptografik algoritmi bilan taqqoslash bajarilgan.

Asimmetrik shifrlash algoritmi Mandelbrot va Julia fraktal ketma-ketliklariga asoslangan. Fraktal ketma-ketlik iteratsion funksiya yordamida olinadi, bu funksiya o‘z navbatida bir tomonlama funksiya hisoblanadi, bunday funksiyalarning bir yo‘nalishli kriptogrammasi boshlang‘ich parametrlar qiymatlarining keng doirasini qayta ko‘rib chiqishsiz samarali tarzda qayta ishlanmaydi. Shu bilan birga, to‘g‘ridan-to‘g‘ri hisoblash ancha oson amalga oshiriladi. Taklif qilingan protokolda yuboruvchi va qabul qiluvchi, almashinuv ishtirokchilari uchun umumiy bo‘lgan murakkab son C va butun son x ni kelishib olishlari va ulardan foydalanishlari kerak. Yuboruvchi va qabul qiluvchi kompleks n va butun e sonidan iborat bo‘lgan, n>x va butun qiymati d bo‘lgan shaxsiy kalitlarini yaratadi. Qabul qiluvchi shaxsiy kalit sifatida n>x bilan kompleks e sonini va n butun sonini yaratadi, jo‘natuvchi esa shaxsiy kalitlari sifatida k kompleks sonini va d butun sonini yaratadi. Yuboruvchi va qabul qiluvchi o‘zlarining yopiq kalitlarini hamda C qiymatini Mandelbrot funksiyasi uchun kirish ma’lumotlari sifatida ishlatib, ochiq kalitlar $Z_n * e$ va $Z_k * d$ ni olishadi, so‘ngra yuboruvchi va qabul qiluvchi ochiq kalitlarni almashishlari kerak. Yuboruvchi qabul qiluvchining ochiq kalitini oladi va o‘zining yopiq kaliti bilan birgalikda uni ishlatib, ma’lumotlarni shifrlash uchun yopiq kalitni hisoblaydi. Keyin shifrlangan ma’lumotlar ochiq kanal orqali qabul qiluvchiga yuboriladi. Qabul qiluvchi, yuboruvchining ochiq kaliti yordamida, o‘z yopiq kalitini hisoblab, olingan shifrlangan ma’lumotlarni deshifrlaydi.

Ochiq va yopiq kalitlarni hisoblash algoritmi quyidagi ifoda asosida amalga oshiriladi:

Yopiq kalit:

$$K = c^{n-x} * q_n * e = c^{k-x} * q_k * d \qquad (1)$$

bu yerda x, n, k butun sonlar; c, e, d, q – kompleks sonlar; q_n, q_k – funksiyaning n va k takrorlanishi natijasi:

$$q_{i+1} = q_i * c * e(d)$$

bu yerda $q_0 = P_{a(b)}$.

1) Yuboruvchi (A) va qabul qiluvchi (B) barcha uchun umumiy bo‘lgan murakkab son c va butun son x ni biladilar, bu qiymatlar sir emas va istagan har bir kishi tomonidan olinishi mumkin;

2) Yuboruvchi (A) sirli kalitni yaratadi, bu kalit (n, e) sonlaridan iborat bo‘lib, n>x va e Mandelbrot to‘plamiga tegishli.

3) Yuboruvchi (A) quyidagi formula bo‘yicha ochiq kalitni hisoblaydi:

$$P_a = Z_n * e$$

bu yerda Z_n - iterativ funksiya.

$$Z_{i+1} = Z_i * c^2 * e$$

bu yerda $Z_0 = c$, takrorlashlar soni n ga teng.

Shundan so‘ng, yuboruvchi (A) qabul qiluvchiga (B) olingan ochiq kalitni yuboradi,

4) Qabul qiluvchi (B) sirli kalitni yaratadi, bu kalit (k, d) sonlaridan iborat bo‘lib, k>x va d Mandelbrot to‘plamiga mansub;

5) Qabul qiluvchi (B) quyidagi formula bo‘yicha ochiq kalitni hisoblaydi:

$$P_b = Z_k * d$$

bu yerda Z_k - iterativ funksiya.

$$Z_{i+1} = Z_i * c^2 * e$$

bu yerda $Z_0 = c$, takrorlashlar soni k ga teng.

Shundan so‘ng, qabul qiluvchi (B) olingan ochiq kalitni yuboruvchi (A) ga yuboradi,

6) Yuboruvchi (A) quyidagi formula bo‘yicha yopiq kalitni hisoblaydi:

$K = c^{n-x} * q_n * e$

bu yerda q_n quyidagiga teng:

$q_{i+1} = q_i * c * e$

bu yerda $q_0 = P_b$ va iteratsiyalar soni n ga teng.

Shundan so‘ng, yuboruvchi (A) xabarni, masalan, "Bir marta ishlatiladigan bloknot" algoritmi yordamida yopiq kalit bilan shifrlaydi va uni qabul qiluvchi(B) ga yuboradi,

7) Qabul qiluvchi (B) quyidagi formula bo‘yicha yopiq kalitni hisoblaydi:

$$K = c^{k-x} * q_n * d$$

bu yerda q_n quyidagiga teng:

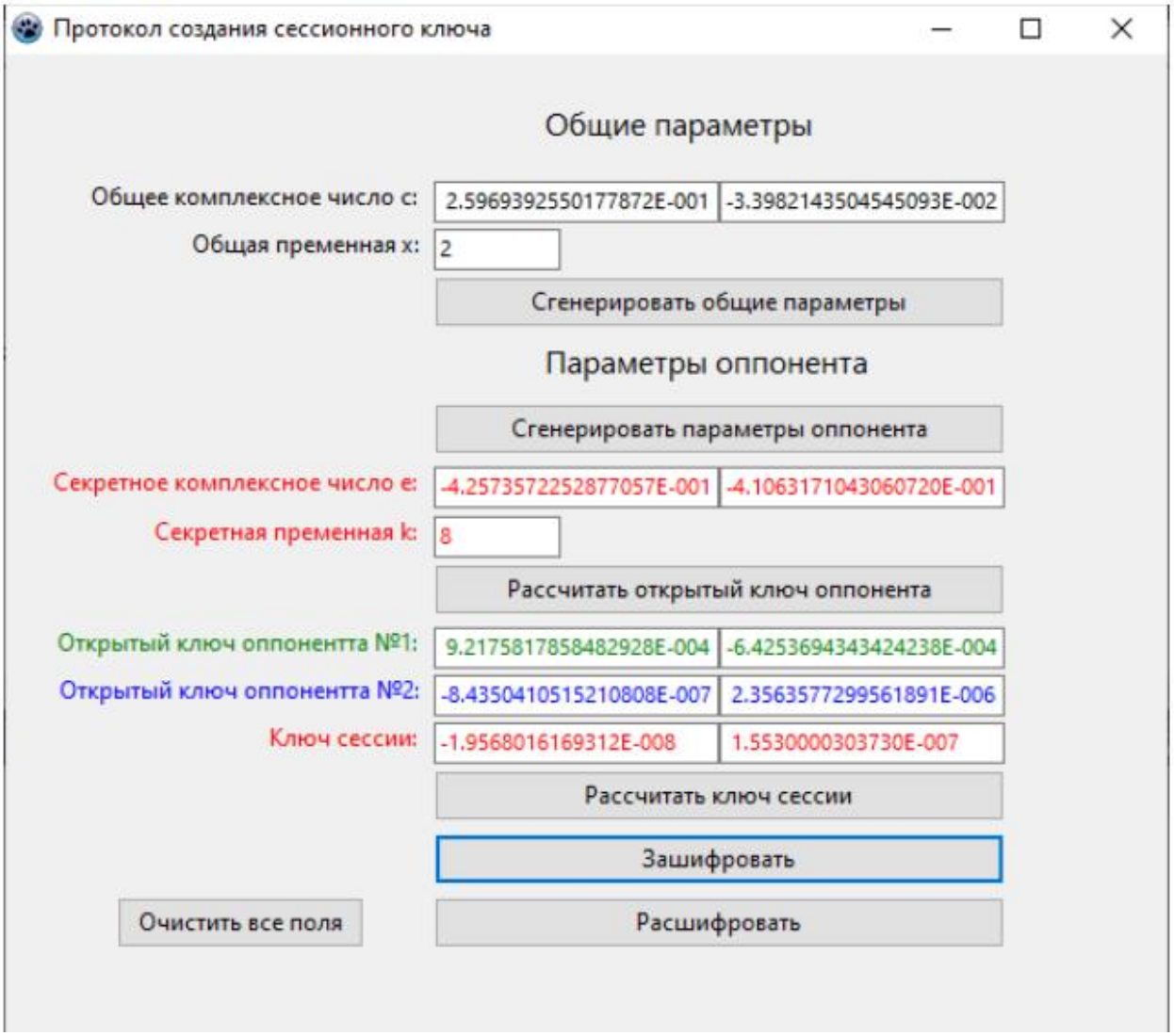
$$q_{i+1} = q_i * c * d$$

bu yerda $q_0 = P_a$ va iteratsiyalar soni k ga teng.

So‘ngra, qabul qiluvchi (B) xabarni xuddi shu algoritm yordamida deshifrlaydi.

Ushbu tadqiqot doirasida fraktal shifrlash algoritmini va ushbu algoritmga qarshi kripto-hujumni amalga oshirish uchun dasturlar yaratildi.

Dastur shuningdek, ma’lumotlarni almashtirish (o‘zgartirish) usuli bilan fayllarni shifrlaydi va yopiq kalit yordamida deshifrlaydi. 1-rasmda fraktal shifrlashni amalga oshiruvchi dasturning interfeysi keltirilgan.



Dastur bilan ishlash algoritmi quyidagilarni o‘z ichiga oladi:

- Ushbu dasturni ikkala raqib ham ishga tushirishi kerak;
- Keyin ikkala raqib ham bir xil umumiy sonlarni tanlashlari kerak: murakkab son c va o‘zgaruvchan x;
- Har bir raqib o‘z dasturida maxfiy o‘zgaruvchilarni e va k generatsiya qiladi;
- "Raqibning ochiq kalitini hisoblash" tugmasini bosish;

- Oldingi bosqichda hosil bo‘lgan murakkab sonni raqibning "Ochiq kaliti № 1" raqibga yuborish;
- Raqibdan olingan ochiq kalitni "Raqibning ochiq kaliti № 2" ustuniga kiritish;
- "Sessiya kalitini hisoblash" tugmasini bosish. Shu paytda shifrlash yoki deshifrlash uchun ishlatiladigan yopiq kalit hisoblanadi;
- Bir raqib shifrlash tugmasini bosadi, shifrlanadigan faylni tanlaydi, so‘ngra shifrlangan faylni saqlaydi. Shifrlangan fayl ikkinchi ishtirokchiga yuboriladi;
- Ikkinchi ishtirokchi ham sessiya kalitini hisoblaydi va "Deshifrlash" tugmasini bosadi, shifrlangan faylni tanlaydi, so‘ng deshifrlangan faylni saqlaydi;
- Natijada ikkinchi ishtirokchi asl faylni oladi.

(1) hisob-kitobni ko‘rib chiqishda, ochiq kalit K ni olish uchun buzg‘unchiga n va e yoki k va d kabi noma’lum o‘zgaruvchilarni hisoblash kerak bo‘ladi. Shuningdek, ushbu asosiy tenglikni bajarish kerak bo‘lgani uchun, to‘rtta sonni to‘g‘ri tanlash zarur.

Bu sonlar $P_a = Z_n * e$ va $P_b = Z_k * d$ ochiq kalitlar mavjud bo‘lib, bu yerda $Z_{i+1} = Z_i * c^2 * e(d),\ z_0 = c.$

Iteratsion jarayonni tahlil qilib, quyidagi qonuniyatlarni topamiz:

$$z_0 = c;\ z_1 = c * c^2 * e = c^3 * e;\ z_2 = c^3 * e * c^2 * e = c^5 * e^2;\ z_3 = c^5 * e^2 * c^2 * e = c^7 * e^3\ .$$

Natijada:

$$z_n = c^{2*n+1} * e^n;\ P_a = c^{2*n+1} * e^{n+1}.$$

Shunda:

$$e^{n+1} = \frac{P_a}{c^{2*n+1}} \Rightarrow e = \sqrt[n+1]{\frac{P_a}{c^{2*n+1}}} \qquad (2)$$

Va shunga o‘xshash:

$$d = \sqrt[k+1]{\frac{P_b}{c^{2*k+1}}} \qquad (3)$$

e va d murakkab sonlar bo‘lganligi sababli, har bir n va k uchun n+1 va k+1 yechim variantlari mavjud. Peribor x+1 dan boshlanadi, shuning uchun bir va shunga o‘xshash boshqa ishtiroklari uchun $\frac{(n+1)*(n+2)}{2} - \frac{(x+1)*(x+2)}{2}$ yechim variantlari bo‘ladi.

Yopiq kalit ikkala ishtirokchi uchun bir xil bo‘lishi kerakligi sababli, $\left(\frac{(n+1)*(n+2)}{2} - \frac{(x+1)*(x+2)}{2}\right) * \left(\frac{(k+1)*(k+2)}{2} - \frac{(x+1)*(x+2)}{2}\right)$ jiddiy o‘zgaruvchilarni ko‘rib chiqish kerak, ularni yopiq kalitni topish formulasiga qo‘yib variantlarni sinab ko‘rish kerak(1).

Masalan, agar n va k 100 dan katta bo‘lsa, x esa kichik bo‘lsa, bu holda allaqachon 25 milliondan ortiq variantlar mavjud bo‘ladi, bu, o‘z navbatida, yetarli darajada

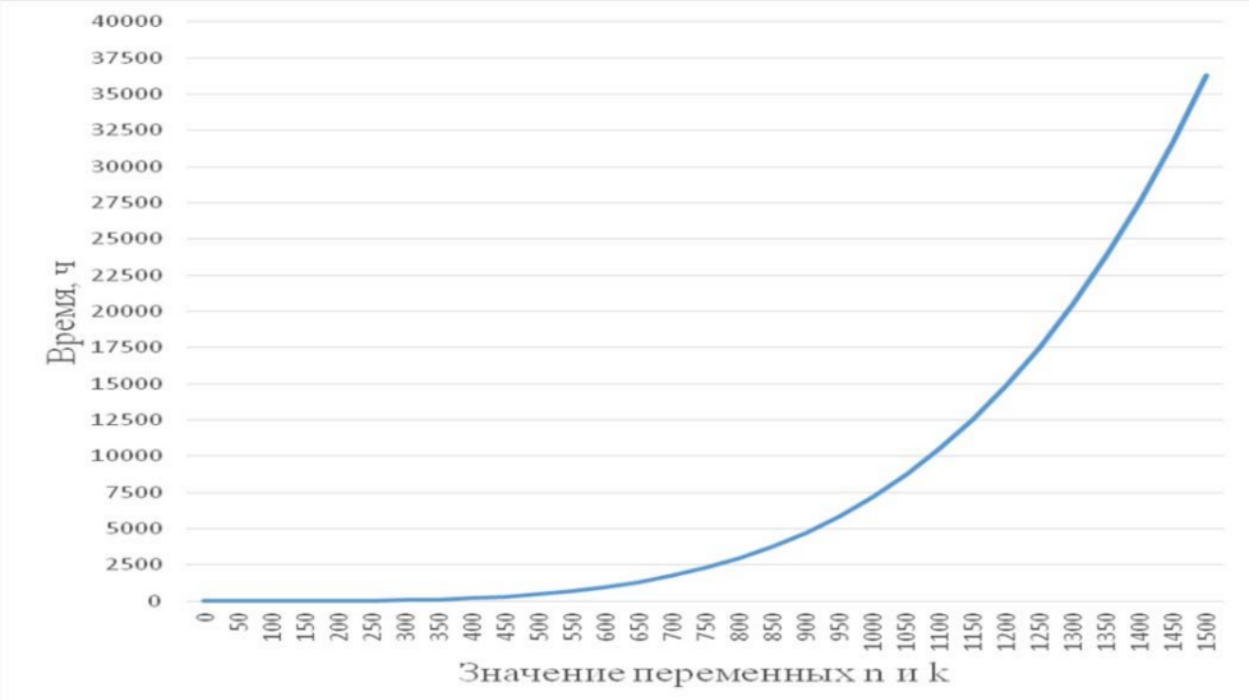
ishonchli ko‘rsatkich emas hisoblanadi. Test tizimida mumkin bo‘lgan kalitlarni to‘liq periborini hisoblash vaqti 44 daqiqa deb belgilangan, bu vaqtni zamonaviy yuqori samarali video kartalar bir necha barobar qisqartirishi mumkin. 2-rasmda n va k o‘zgaruvchilari qiymatlariga bog'liq holda kalitlarni peribor qilish vaqtining bog'liqligi ko‘rsatilgan. Ushbu bog'liqlikni tahlil qilish orqali, o‘zgaruvchilarning qiymati ortishi bilan kerakli vaqt nisbatan o‘zgarmasligini ko‘rish mumkin, masalan n va k qiymatlarini besh marta oshirish hisoblash vaqtini deyarli 615 marta oshiradi.

(2 va 3) ifodalarga asoslanib, bir raqibning maxfiy kalitini tanlash uchun dastur yozilgan. Dastur kirishda umumiy o‘zgaruvchilar c va x ni, shuningdek bir raqibning ochiq kalitini qabul qiladi. k > x bo‘lgan butun sonlar peribori usulida dastur mumkin bo‘lgan kalitlarni chiqaradi.

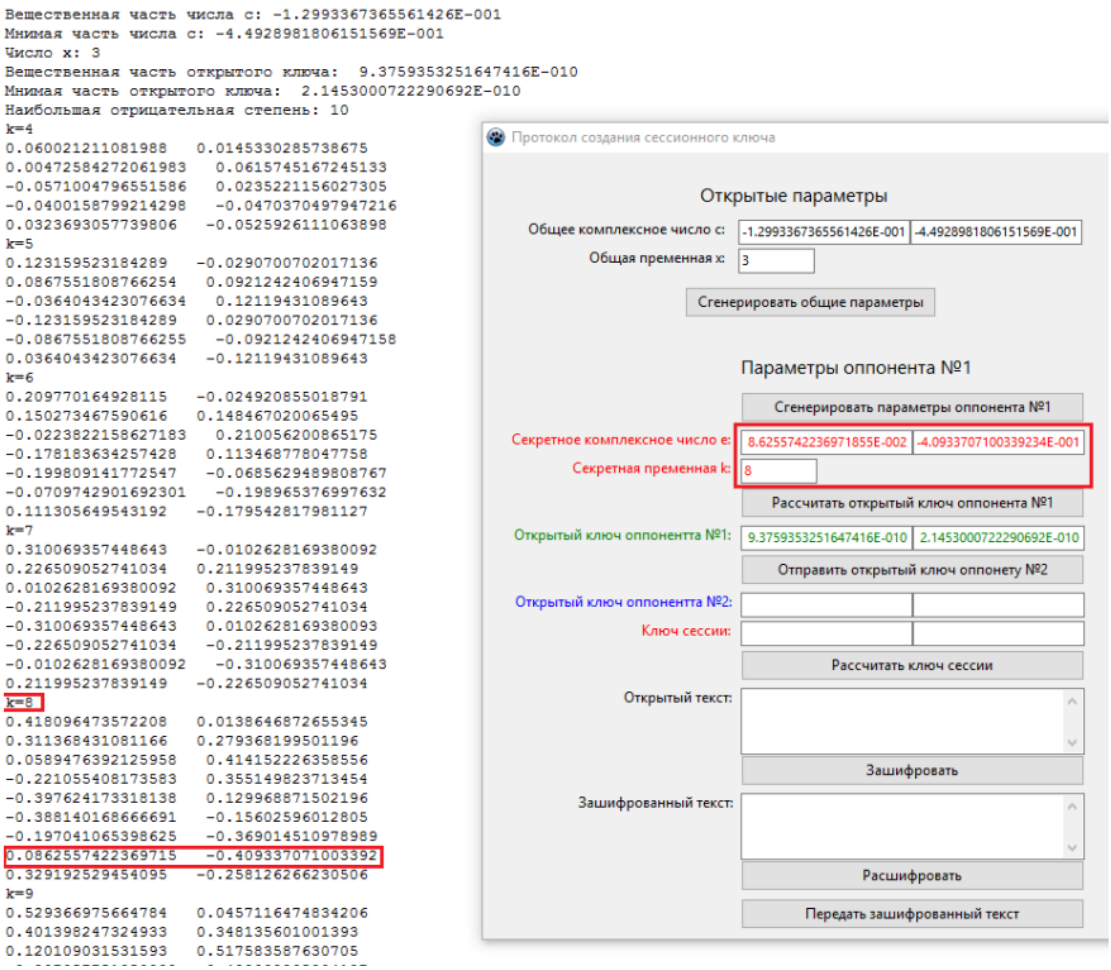
Dasturning ishlashi misoli 3-rasmda ko‘rsatilgan. Masalan, boshlang'ich shifrlashda k = 8, x = 3 bo‘lganida, bir ishtirokchi uchun jami 35 ta variant mavjudю

Mandelbrot to‘plami tahlili natijasida algoritmni yaxshilash bo‘yicha quyidagi taklif kiritilgan.

Murakkab sonni hisoblashning aniqligi cheklanganligi sababli, ketma-ketlik bir nuqtada yig'ilganda, avvalgi qiymat haqidagi ma'lumotlarning bir qismi yo‘qoladi, hatto oldingi qadamning to‘liq takrorlanishigacha. Shuningdek, nuqta to‘plamning chegarasidan qanchalik uzoq bo‘lsa, u shunchalik tez biror muayyan stasionar qiymatga intilishini kuzatish mumkin.



2-rasm. Kalitlarning to‘liq periborini bajarish vaqtining n va k maxfiy o‘zgaruvchilari qiymatlariga bog'liqligi grafigi.



3-rasm. Chap tomonda ishga tushirilgan parol tanlash dasturining chiqish ma'lumotlari, o‘ng tomonda shifrlash dasturi ko‘rsatilgan.

Ta'kidlash joizki, agar nuqta bir qancha iteratsiyalardan so‘ng to‘liq takrorlangan bo‘lsa (cheklangan aniqlik tufayli), u holda u iteratsiyalar soni haqida va aniq boshlang'ich qiymat haqida ma'lumotni yo‘qotgan bo‘lishi mumkin. Ushbu taxmin, tegishli tekshiruvlardan so‘ng, kriptografik algoritmlarda qo‘llanilishi mumkin.

Masalan, agar fraktalni psevdotasodifiy sonlar ketma-ketligini yaratish uchun ishlatilsa («bir marta ishlatiladigan bloknot» uchun), boshlang'ich qiymat fraktalning chegarasiga yaqin bo‘lishi ma'qul, shunda ketma-ketlik uzoq vaqt takrorlanmaydi. Shuningdek, ushbu takrorlanish belgisiga ko‘ra tasodifiy sonlarni tanlash tavsiya etiladi (kompyuterda hisob-kitoblarning cheklovlari sababli, o‘zi ketma-ketlik cheksizdir).

Ushbu ishda taqdim etilgan algoritm uchun, aksincha, ketma-ketlik takrorlanganda, boshlang‘ich qiymat haqidagi ma’lumotlar yo‘qoladi. Shuning uchun, teskari amallarni bajarib, boshlang‘ich qiymatni topish imkoni mavjud emas. Faqat murakkab sonlar va iteratsiyalar sonining qo‘pol peribori mumkin bo‘ladi. Yakunda, kalit fazosi o‘lchamining bahosini olishimiz mumkin: murakkab son ikkita

o‘zgaruvchan nuqtali sonlardan iborat bo‘lib, iteratsiyalar soni butun bo‘lgani uchun, kalit 64 + 64 + 32 bit bo‘ladi, bu esa 2^{160} kalit variantlarini anglatadi.

Shu sababli, taklif etilayotgan yaxshilash usuli quyidagicha: maxfiy sonlarni yaratish bosqichida ushbu algoritm uchun zaif sonlarni chetlab o‘tish. Ketma-ketlik belgilangan iteratsiyalar sonidan biroz oldin takrorlanishi kerak. Buning uchun har bir iteratsiyada funksiya qiymatini eslab qolish va takrorlanishini tekshirish kerak. Agar son takrorlanmasa, yangi son yaratish zarur. Shuningdek, dastlabki bosqichlardagi takrorlanishni oldini olish kerak. Algoritmning mustahkamligini oshirishning yana bir usuli yangi maxfiy o‘zgaruvchini qo‘shish bo‘lib, u e o‘zgaruvchisining qiymatini hisoblab chiqish imkoniyatini bermaydi. Shuningdek, kalitlarni peribor qiluvchi dastur asl maxfiy sonni aniq aniqlay olmadi, 15 ta ma’no qoldiqlaridan sezilarli farq qiladi, hatto yaxlitlash hisobga olinsa ham. Bu, yaqin kalitlarni qayta peribor qilishga olib keladi.

Shunday qilib, n sonini (iteratsiyalar soni) tanlash orqali hujum qilish va maxfiy murakkab sonni hisoblashning iloji bo‘lmasligi uchun, maxsus murakkab sonni tanlash kerak. Bu son fraktal funksiyasi oxirgi iteratsiyada kompyuter tomonidan sonlarni hisoblashdagi cheklangan aniqlik tufayli yetarli ma'lumotni yo‘qotishini ta'minlashi kerak, bu esa taklif etilgan hujum algoritmini amalga oshirish imkoniyatini berkitadi.

Natijada, faqat barcha mumkin bo‘lgan maxfiy sonlarning to‘liq peribori bilan buzish mumkin bo‘ladi. Funktsiya dastlabki ma'lumotni yo‘qotishi uchun, uning qiymatlari oxirgi bosqichlarda takrorlanishni boshlashi kifoya.

Bundan tashqari, kalitlarni hisoblash jarayonida ishtirok etuvchi yana bir maxfiy murakkab o‘zgaruvchi e1 kiritildi, bu esa funksiya iteratsiyalarining mumkin bo‘lgan soni va maxfiy o‘zgaruvchilarning mumkin bo‘lgan qiymati haqida ma'lumotni to‘liq yo‘q qilish imkonini beradi (faqat e va e1 mahsulotini hisoblash mumkin).

Natijada tasodifiy son hosil bo‘ladi, bu son shartlarni qanoatlantiradi va oddiy hisoblash yordamida buzib bo‘lmaydigan bo‘ladi.

Fraktal shifrlash algoritmini amalga oshirish, bilimlarni o‘rganish va mustahkamlash nuqtai nazaridan, shuningdek, fan sifatida umuman katta qiziqish uyg'otadi.

Kriptografiya yangi algoritmlar va ma'lumotlarni himoya qilish usullarini yaratish va o‘rganishga doimiy ehtiyoj sezadi, chunki hisoblash texnikasi va shifrlangan ma'lumotlarni buzish usullarining rivojlanishi mavjud himoya usullarining qarshilik darajasini pasaytiradi.

Foydalanilgan adabiyotlar

1. Кулешов С.В. Фрактальное шифрование. Тр. СПИИРАН, 2004. Вып. 2. Т. 1. С. 231 235.
2. Синьковский А.В. Разработка эффективных методов решений по защите информа ции с использованием фрактального моделирования в условиях

автоматизированного проекти рования и производства. М.: МГТУ «СТАНКИН», 2007. 183 с.

3. Rubesh Anand P.M., Gaurav Bajpai, Bhaskar V., Real-Time Summetric Cryptography using Quaternion Julia Set // International Journal of Computer Science and Network Security, VOL.9 No.3ю March 2009. 7 p.
4. Shafali Agarwal, Ashish Negi, A key agreement protocol based on superior fractal sets // International Journal of Advances in Applied Sciences (IJAAS) Vol. 3, No. 2, 2014. P. 82– 86.
5. Ojha1 D.B., Shree Ms., Dwivedi A., Mishra A. An Approach for Embedding Elliptic Curve in Fractal Based Digital Signature Scheme // Journal of scientific research, 2011. P. 75– 79.
6. Mohammad Ahmad Alia, Azman Bin Samsudin. A New Public-Key Cryptosystem Based on Mandelbrot and Julia Fractal Sets // Asian Joumal of Information Technology, 2007. P. 567– 575.
7. Мандельброт Б. Фрактальная геометрия природы. М.: Институт компьютерных ис следований, 2002. 656 с.