**13- amaliy ish**

**Mavzu: Ketma-ketliklarni tasodifiylikka tekshirishda NIST statistik testlar to‘plamidan foydalanish**

**Ishdan maqsad**: Ketma-ketliklarni tasodifiylikka tekshirishda NIST statistik testlar to‘plami haqida bilim ko‘nikmalarga ega bo‘lish

**Nazariy**

Mavjud blokli simmetrik shifrlash algoritmlari DES, AES, GOST 28147-89 mos ravishda 56 bit, 128 bit, yoki 256 bit, yoki 512 bit va 256 bit uzunlikdagi oldindan belgilab qo‘yilgan qoida bo‘yicha generatsiya qilingan kalitlardan foydalanadi. Biroq standart algoritmlarda belgilab qo‘yilgan qoida bo‘yicha generatsiya qilingan barcha kalitlar har doim ham shifrmatnni o’chish maqsadida ochiq aloqa tarmog‘ini nazorat qiluvchi kriptoanalitik tomonidan uyushtiriladigan turli kriptohujumlarga bardoshli bo‘lmasligi mumkin. Masalan, kalitni tashkil etuvchi bitlar ketma-ketligi faqat nollardan yoki birlardan yoki bo‘lmasa, nol va birlarning kombinatsiyam fiksirlangan davr bilan takrorlanishi yordamida tuzilgan bo‘lsa, bu toifa kalitlar bardoshsiz hisoblanadi. Chunki ushbu tur bitlar ketma-ketligida, shu ketma-ketlikni tashkil etuvchi nol va bir elementlari davriy takrorlanishining matematik qonuniyatini oldindan aytish imkoniyati mavjud. U holda bu kabi generatsiya qilingan bitlar ketma-ketligidan simmetrik shifrlash algoritmlari uchun maxfiy kalit sifatida foydalanish maqsadga muvofiq emas. Demak, yuqoridagi fikr-muloxazalardan kelib chiqib, «kriptoalgoritmlar maxfiy kalit bloklari uchun tasodifiy bitlar ketma- ketligi qanday quriladi?» degan savolning tug‘ilishi tabiiy, yani agar biror qoida bo‘yicha kalit blokining k=k1 k2..km , ketma-ketligi olingan bo‘lsa, bu yerda k∊ {0,1}, va m = 56, 128, 192, 256 bo‘lishi mumkin. U holda kalit blokida ki. - bitlarning taqsimoti tasodifiy yoki tasodifiy emasligi qanday aniqlanadi? Ushbu savolga javob olish uchun kalit blokida ki. - bitlarning taqsimotini amaliyotda keng tarqalgan va boshqa mavjud tasodifiylik testlarining asoslarini tashkil etuvchi «Xi-kvadrat» taqsimotidan foydalanib aniqlash kerak bo‘ladi.

Tasodifiylikka tekshiruvchi testlar 2 xil bo‘ladi:

Grafik testlar - grafik testlar foydalanuvchiga tekshirilayotgan ketma-ketlikning ma’lum bir grafik bog‘liqligi haqidagi ma’lumotni berib, u bo‘yicha tekshirilayotgan ketma-ketlik xossalari to’g’risida xulosa chiqarish imkoniyatini beradi.

Baholash testlari - baholash testlari tekshirilayotgan ketma- ketlik statistik xossalarini tahlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi :



13.1- rasm. Tasodifiylik darajasini aniqlovchi testlar

Kalit blokini tashkil etuvchi belgilar taqsimotini tasodifiylikka tekshirishda, avvalo, bu kalit blokini biror qoida bo‘yicha hosil qilib olish zarur. Bu kabi ishlar, odatda, psevdotasodifiy ketma-ketliklar generatorlari orqali amalga oshiriladi. Psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar haqida, ularning tuzilish asoslariga ko’ra turkumlari, xususiyatlari, xossalari, kriptografik masalarni yechishdagi qo’llanishlari yuqorida batafsil tahlil qilingan. Xususan:

* + 1. Chiziqli kongruent;
    2. Kvadratik kongruent;
    3. Bir tomonlama unikatsiyalarga, shifrlash va xeshlash algoritmlariga asoslangan;
    4. Sonlar nazariyasi muammolariga asoslangan generatorlar tahlil qilingan.

Taqsimotni tasodifiylikka tekshirishning «Xi-kvadrat» kriteriysi

Biror o’tkazilayotgan tajriba natijalarining barcha mumkin bo‘lgan holatlari *,* ,……. dan iborat va ularning soni *k* ga teng bo‘lib, bu tajriba bir-biriga bog‘liqsiz holda n marta o’tkazilsin.. Shunda,*,* ,…….- holatlarni, ularning *n* marta o’tkazilgan tajribada, bir xil sonda takrorlanishidan (tekis taqsimotdan yoki bir xil chastotaga ega bo‘lishdan) qanchalik chetlanganligini baholash masalasini yechilishini ko‘rib o’tiladi. Buning uchun quyidagicha belgilashlar kiritiladi:

- eksperiment natijasi bo‘lishining Ehtimollik qiymati;

- eksperiment natijalarining holatga tegishlilari (tenglari) soni.

U holda, bu belgilashlarga nisbatan «Xi-kvadarat» deb ataluvchi taqsimot kriteriysi ushbu

*V = ,*

formula orqali aniqlanadi.

Agar tajriba *n* martadan bir necha marta o‘tkazilganda, har doim *,*,…….holatlar teng . martadan takrorlansa (tekis taqsimlangan yoki bir xil chastotali bo‘lsa), ya’ni *,*,……. bo‘lsa, u holda =*= …..==* deb xulosa qilinadi va

*V = ==0*

tenglik o‘rinli bo‘ladi. Bunday jarayonning ilmiy tadqiqot uchun qizig‘i yo‘q. Ammo, amaldagi aksariyat jarayonlarda bunday holat kuzatilmaydi, ya’ni biror tajriba bir-biriga bog‘liqsiz ravishda *n* marta o‘tkazilganda: *,=* ,=…….= = holat kuzatilmaydi. Shuning uchun *,* ,……., holatlarni ro‘y berish Ehtimolliklari bir xil =*= …..==* bo‘lib, bir-biriga bog‘liq bo’lmagan ravishda p marta o’tkazilganda, bu holatlarning ro‘y berishi soni mos ravishda

*,* ,……. bo‘lsa, u holda ushbu

*V = =*

formula *,=* ,=…….= = bo‘lgan teng taqsimotdan *,=* ,=…….= – teng bo’lmagan taqsimoqni o‘rtacha kvardatik chetlanishni ifodalaydi. Bu oxirgi formuladagi () - ifoda biror o’zgarmas son bilan chegaralangan, ya’ni | | *C*= const.

*V = == → 0, n* bo‘lsa.

Bu oxirgi formuladan, biror generator orqali hosil qilingan psevdotasodifiy ketma-ketlikning davri yetarli uzun bo‘lib, barcha mumkin bo‘lgan bitlar, baytlar va qism bloklarining taqsimoti deyarli tekis (teng taksimlangan) bo‘lsa, u holda «Xi-kvadarat» taqsimot kriteriysining bu ketma-ketlikka nisbatan qiymati nolga yaqin bo‘lib, uning tasodifiylik darajasi yuqori hisoblanadi.

Quyida esa standart DES, GOST 28147-89, AES-FIPS-197 va boshqa simmetrik shifrlash algoritmlari uchun maxfiy kalitni tasodifiy qilib generatsiya qilishning Xi-kvadrat taqsimoti orqali qanday amalga oshirilishini ko‘rib o’tamiz.

Berilgan kalit bloki bo‘yicha quyidagi jadvalni tuzib olamiz:

Qiymat (s): 0 1;

Ehtimollik () : ;

Kuzatilayotgan son (): ,

bu yerda: va mos ravishda kalit blokida ishtirok etuvchi nollar va birlar, +, orqali kalit uzunligini belgilaydi, masalan ;

kutilayotgan son (n\*) : ;

Xi-kvadrat taqsimoti formulasi bo‘yicha [10]:

*V =* hisoblanadi

Ushbu qaralayotgan holatda:

k=2; 5 = 0,1; ; =; =; ; u holda, quyidagicha

kattalikka ega bo’lamiz:

*V =*

Bu kattalikni hisoblash uchun bizga Xi-kvadrat taqsimotining kritik nuqtalari jadvali deb ataluvchi jadval kerak bo‘ladi.

13.1- jadval

Xi –kvadrat taqsimotining kritik nuqtalari jadvali

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | p=1% | p=5% | p=25% | p=50% | p=75% | p=95% | p=99% |
| N=1 | 0.00016 | 0.00393 | 0.1015 | 0.4549 | 1.323 | 3.841 | 6.635 |
| N=2 | 0.02010 | 0.1026 | 0.5754 | 1.386 | 2.773 | 5.991 | 9.210 |
| N =3 | 0.1148 | 0.3518 | 1.213 | 2.366 | 4.108 | 7.815 | 11.34 |
| N =4 | 0.2971 | 0.7107 | 1.923 | 3.357 | 5.385 | 9.488 | 13.28 |
| N =5 | 0.5543 | 1.1455 | 2.675 | 4.351 | 6.626 | 11.07 | 15.09 |
| N =6 | 0.8721 | 1.635 | 3.455 | 5.348 | 7.841 | 12.59 | 16.81 |
| N =7 | 1.239 | 2.167 | 4.255 | 6.346 | 9.037 | 14.07 | 18.48 |
| N =8 | 1.646 | 2.733 | 5.071 | 7.344 | 10.22 | 15.21 | 20.09 |
| N =9 | 2.088 | 3.325 | 5.899 | 8.343 | 11.39 | 16.92 | 21.67 |
| N =10 | 2.558 | 3.940 | 6.737 | 9.342 | 12.55 | 18.31 | 23.21 |
| N =11 | 3.053 | 4.575 | 7.584 | 10.34 | 13.70 | 19.68 | 24.72 |
| N =12 | 3.571 | 5.226 | 8.438 | 11.34 | 14.85 | 21.03 | 26.22 |
| N =15 | 5.229 | 7.261 | 11.04 | 14.34 | 18.25 | 25.00 | 30.58 |
| N =20 | 8.260 | 10.585 | 15.45 | 19.34 | 23.83 | 31.41 | 37.57 |
| N =30 | 14.95 | 18.49 | 24.48 | 29.34 | 34.80 | 43.77 | 50.89 |
| N =50 | 29.71 | 34.76 | 42.94 | 49.33 | 56.33 | 67.50 | 76.15 |
| N >30 | V+ + –o () | | | | | | |
| =8 | -2.33 | -1.36 | -0.674 | 0.00 | 0.674 | 1.64 | 2.33 |

«Xi-kvadrat» kriteriysi jadvali v=k:-l =2-1 = 1, satridan *v* qiymat joylashish Oraliqini topamiz. Agar v qiymat jadval ustunining p = 25% dan p = 25%, Oraliqida bo‘lsa, u holda psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma- ketligi tasodifiy deb olinadi.

Garchand psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma-ketligi tasodifiylikka «Xi-kvadrat» kriteriysi bo‘yicha tekshirilganda ijobiy javob olingan bo‘lsa ham, undan ko‘ra ishonchli va mukammal bo‘lgan javob olish uchun qaralayotgan bitlar ketma-ketligini boshqa mavjud tasodifiylik testlariga ham tekshirib ko’rish lozim.

Aytaylik, psevotasodifiy generator yordamida hosil qilingan kalit bloki: k=*,*,……. *=,*,…….*,* bu yerda {0; 1}

yuqorida keltirilgan kriteriy bo‘yicha tasodifiylikka tekshirilgan va qoniqarli javob olingan. Amaliyot jarayonida shifrtizimlar bilan ishlashda aniqlangan bardoshsiz kalitlarni k=*,*,…….kabi belgilaymiz.

Psevotasodifiy generator yordamida hosil qilingan kalit bloki: k=*,*,……. *=,*,…….*,* va amaliyot jarayonida bardoshsiz deb topilgan k=*,*,……. *,*  kalitlarning farqi ko‘rib o’tiladi:

= k = (1) (1)….. (1) bu farq bo‘yicha mos ravishda 0 va 1 bitlar soni (1) ; (1);

= k = (2) (2)….. (2) bu farq bo‘yicha mos ravishda 0 va 1 bitlar soni (2) ; (2);

= k = (m) (m)….. (m) bu farq bo‘yicha mos ravishda 0 va 1 bitlar soni (m) ; (m); bu kattaliklardan foydalangan holda, quyidagilarni xisoblaymiz:

*=*

*=*

*=*

V=

«Xi-kvadrat» kriteriysi jadvali v=k-1=2-1 = 1, satridan V qiymat joylashish Oraliqini topamiz. Agar V qiymat jadval ustunining p = 25% dan p= 25%, Oraliqida bo‘lsa, u holda psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma- ketligi tasodifiy deb olinadi.

**Topshiriq**

Taqsimotni tasodifiylikka tekshirishning «Xi-kvadrat» ishlash funksiyasi qadamma – qadam izohlansin.

Nazorat savollari

1. Taqsimotni tasodifiylikka tekshirishning «Xi-kvadrat» kriteriysi tasnifi
2. Tasodifiylik darajasini aniqlovchi testlar turlari
3. Psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar tasnifi

**14- amaliy ish**

**Mavzu: Openssl kutubxonasidan foydalangan holda ma’lumotlarni xesh qiymatini hisoblash**

**Ishdan maqsad**: Xeshlash algoritmining ishlatilish sohalari va ishlash prinsiplari haqida amaliy bilim ko‘nikmalarga ega bo‘lish.

**Nazariy qism**

Kriptografiyada, xesh funksiya deb ixtiyoriy uzunlikdagi (bitlar yoki baytlar birliklarida) ma’lumotni biror fiksirlangan (belgilangan) uzunlikdagi (bitlar yoki baytlar birliklariga) qiymatga o‘tkazib beruvchi funksiyaga aytiladi. Xesh funksiyalardan amalda statistik tajribalar o‘tkazishda, mantiqiy qurilmalarni tekshirishda, ma’lumotlar bazasida tez qidirib topish algoritmlarini yaratishda va ma’lumotlar bazasidagi ma’lumotlarning butunligini tekshirishda foydalaniladi.

Xesh funksiya deb, ixtiyoriy uzunlikdagi M ma’lumotni fiksirlangan uzunlikdagi h(M)=H qiymatga akslantib beruvchi, oson hisoblanadigan bir tomonli funksiyaga aytiladi.

Xesh qiymat: “xesh qiymat”, “svertka”, “daydjest”, “barmoq izlari” deb ham ataladi.

Xesh funksiyaga nisbatan quyidagi talablar qo‘yiladi:

1. Ixtiyoriy uzunlikdagi matn uchun qo‘llab bo‘lishlik.

2. Chiqishda belgilangan uzunlikdagi qiymatni berishlik.

3. Ixtiyoriy berilgan x bo‘yicha h(x) oson hisoblanishlik.

4. Ixtiyoriy berilgan H bo‘yicha h (x)= N tenglikdan x ni hisoblab topib bo‘lmaslik. (Bir tomonlilik xususiyati).

5. Olingan x va y≠x matnlar uchun h(x)≠ h(y) munosabat o‘rinli bo‘lishi. (Kolliziyaga bardoshlilik xususiyati).

**MD 5 xesh funksiyasi.** MD5 algoritmda kiruvchi ma’lumot uzunligi ixtiyoriy bo‘lib, xesh qiymat uzunligi 128 bit bo‘ladi. MD 5 xesh funksiyasi algoritmida kiruvchi ma’lumot 512 bitlik bloklarga ajratilib, ular 16 ta 32 bitlik qism bloklarga ajratiladi va bular ustida amallar bajariladi.

Faraz qilaylik, bizga uzunligi b bit bo‘lgan, bu yerda b – ixtiyoriy nomanfiy butun son, ma’lumot berilgan bo‘lsin va bu ma’lumotning bitlari *m0 m1 … m(b-1)* tartibda yozilgan bo‘lsin.

Xesh qiymatni hisoblash uchun quyidagi beshta bosqich bajariladi:

1- bosqich. To‘ldirish bitlarini qo‘shish

Berilgan ma’lumot uzunligi 512 modul bo‘yicha 448 bilan taqqoslanadigan (ma’lumot uzunligi 448 mod 512) qilib to‘ldiriladi, ya’ni, kengaytirilgan ma’lumotning uzunligi unga eng yaqin bo‘lgan 512 ga karrali bo‘lgan sondan 64 bitga kichik bo‘lishi kerak. To‘ldirish hamma vaqt, hattoki ma’lumot uzunligi 512 modul bo‘yicha 448 bilan taqqoslanadigan bo‘lsa ham bajariladi.

To‘ldirish quyidagi tartibda amalga oshiriladi: ma’lumotga 1 ga teng bo‘lgan bitta bit qo‘shiladi, qolgan bitlar esa 0 lar bilan to‘ldiriladi. Shuning uchun qo‘shilgan bitlar soni 1 dan 512 tagacha bo‘ladi.

2- bosqich. Ma’lumotning uzunligini qo‘shish

1-bosqichning natijasiga berilgan ma’lumot uzunligining 64 bitlik qiymati qo‘shiladi. Agar ma’lumotning uzunligi 264 bitdan katta bo‘lsa, bu uzunlik mod 264 bo‘yicha olinib qo‘shiladi.

Shunday qilib, birinchi ikkita bosqich bajarilgandan keyin uzunligi 512 bitga karrali bo‘lgan ma’lumot olinadi, ya’ni kengaytirilgan ma’lumot uzunligi 16 ta 32 bitlik so‘zdan iborat blok uzunligiga karrali bo‘ladi. Natijada hosil qilingan ma’lumotning so‘zlarini M[0, ..., N-1] orqali belgilaymiz, u holda N soni 16 ga karrali bo‘ladi. Shunday qilib, N=L 16 bo‘ladi.

1000...000

Ma’lumot

К bit

L×512 bit=N×32 bit

To‘ldirish (1 dan 512bitgacha)

Ma’lumot uzunligi

(К mod 264)

3- bosqich. Xesh qiymat uchun bufer initsializatsiya qilish

Xesh funksiyaning oraliq va oxirgi natijalarini saqlash uchun 128 bitlik buferdan foydalaniladi. Bu buferni to‘rtta 32 bitlik A, B, C, D registrlar ko‘rinishida tasvirlash mumkin. Bu registrlarga 16 lik sanoq sistemasida quyidagi boshlang‘ich qiymatlar beriladi:

A=0x01234567

B=0x89ABCDEF

C=0xFEDCBA98

D=0x76543210 .

4- bosqich. Ma’lumotni 512 bitlik bloklarga ajratib qayta ishlash

Argumenti va qiymati 32 bitlik so‘z bo‘ladigan to‘rtta yordamchi funksiyani aniqlaymiz:

F(X,Y,Z) = (XY)  ( ⎤ X Z)

G(X,Y,Z) = (XZ) (Y ⎤ Z)

H(X,Y,Z) = X ⊕ Y ⊕ Z

I(X,Y,Z) = Y ⊕ (X  ⎤ Z)

Bu yerda bitlar bo‘yicha mantiqiy AND, OR, NOT, XOR amallari mos ravishda , , ⎤ , ⊕ belgilari bilan ifodalangan.

Bu bosqichda sinus funksiyasi asosida 64 ta so‘zdan qurilgan T[1,…,64] jadvaldan foydalaniladi. T[*i*]=[4294967296×abs(sin(*i*))] bo‘lib, jadvalning *i*–elementini ifodalaydi.Bu yerda[q]ifodaqsonning butun qisminibildiradi, *i* esa radianlarda ifodalangan.

Ushbu bosqichda quyidagi amallar bajariladi:

/\* Har bir 16 so‘zlik blok qayta ishlanadi. \*/

for *I* = 0 to N/16 – 1 do

/\* *i*- блок X га ёзиб олинади. \*/

For *j* = 0 to 15 do

X[*j*] = M[*i*\*16 + *j*].

/\* A ning qiymati AA ga, B ning qiymati BB ga, C ning qiymati CC ga, D ning qiymati DD ga yozib olinadi. \*/

1. = A
2. = B
3. = C
4. =D /\* 1-qadam. \*/

/\* [*abcd k s i*] ifoda quyidagi amalni bildiradi:

*a* = *b* + ((*a+* F(*b*,*c*,*d*) +X[*k*] +T[*i*]) <<< *s*). \*/

\*/ /\* Quyidagi 16 ta amal bajariladi. \*/

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [ABCD 0 7 | 1] | [DABC | 1 12 | 2] | [CDAB 2 17 | | 3] | [BCDA 3 22 | 4] |
| [ABCD 4 7 | 5] | [DABC | 5 12 | 6] | [CDAB 6 17 | | 7] | [BCDA 7 22 | 8] |
| [ABCD 8 7 | 9] | [DABC | 9 12 10] | | [CDAB | 10 17 | 11] | [BCDA 11 22 12] | |
| [ABCD 12 7 13] [DABC 13 12 14] [CDAB | | | | | | 14 17 | 15] | [BCDA 15 22 16] | |

/\* 2-qadam. \*/

/\* [*abcd k s i*] ifoda quyidagi amalni bildiradi:

*a* = *b*+ ((*a* + G(*b*,*c*,*d*) +X[*k*] +T[*i*]) <<< *s*). \*/

\*/ /\* Quyidagi 16 ta amal bajariladi.\*/

[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20] [ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24] [ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28] [ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

/\* 3-qadam. \*/

/\* [*abcd k s i*] ifoda quyidagi amalni bildiradi:

*a* = *b* + ((*a* + H(*b*,*c*,*d*)+ X[*k*] + T[*i*]) <<< *s*). \*/

\*/ /\* Quyidagi 16 ta amal bajariladi.\*/

[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36] [ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40] [ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]

[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48] /\* 4-qadam. \*/

1-қадам

3-қадам

4-қадам

2-қадам

А

В

С

D



MD 5 алгоритмидаги асосий цикл.

/\* [*abcd k s i*] ifoda quyidagi amalni bildiradi:

*a* = *b* + ((*a* + I(*b*,*c*,*d*) + X[*k*] + T[*i*]) <<< *s*). \*/

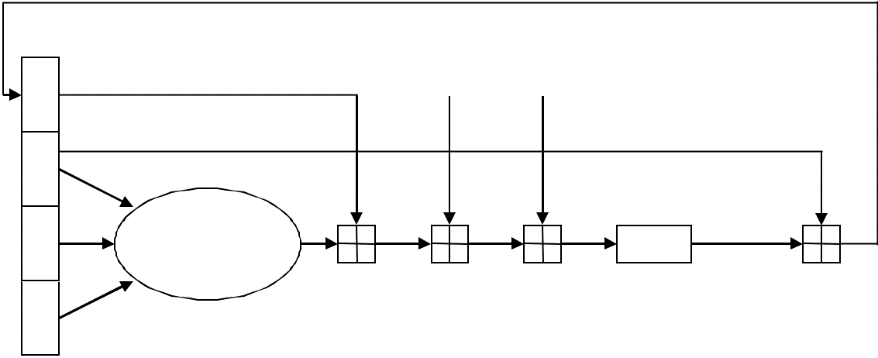
\*/ /\* Quyidagi 16 ta amal bajariladi. \*/

[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52] [ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56] [ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60] [ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]

/\* Quyidagi qo‘shish amali bajariladi. \*/ A=A+AA

B=B+BB C=C+CC D=D+DD

end /\* *I* bo‘yicha sikl \*/



14.1- rasm. MD 5 algoritmida bitta registr qiymatini hisoblash

5- bosqich. Natija

Ma’lumotning xesh qiymati A, B, C, D registrlardagi qiymatlarni birlashtirish natijasida hosil qilinadi.

1-qadam

3-qadam

4-qadam

2-qadam

А

В

С

D



14.2- rasm. MD 5 algoritmidagi asosiy sikl

**SHA algoritm**. SHA algoritmda kiruvchi ma’lumotning uzunligi 264 bitdan kichik bo‘lib, xesh qiymat uzunligi 160 bit bo‘ladi. Kiritilayotgan ma’lumot 512 bitlik bloklarga ajratilib qayta ishlanadi.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

*1-bosqich. To‘ldirish bitlarini qo‘shish.*

Berilgan ma’lumot uzunligi 512 modul bo‘yicha 448 bilan taqqoslanadigan (ma’lumot uzunligi 448 mod 512) qilib to‘ldiriladi. To‘ldirish hamma vaqt, hattoki ma’lumot uzunligi 512 modul bo‘yicha 448 bilan taqqoslanadigan bo‘lsa ham bajariladi.

To‘ldirish quyidagi tartibda amalga oshiriladi: ma’lumotga 1 ga teng bo‘lgan bitta bit qo‘shiladi, qolgan bitlar esa 0 lar bilan to‘ldiriladi. Shuning uchun qo‘shilgan bitlar soni 1 dan 512 tagacha bo‘ladi.

*2- bosqich. Ma’lumotning uzunligini qo‘shish.*

1-bosqichning natijasiga berilgan ma’lumot uzunligining 64 bitlik qiymati qo‘shiladi.

*3- bosqich. Xesh qiymat uchun bufer initsializatsiya qilish.*

Xesh funksiyaning oraliq va oxirgi natijalarini saqlash uchun 160 bitlik buferdan foydalaniladi. Bu buferni beshta 32 bitlik A, B, C, D, Ye registrlar ko‘rinishida tasvirlash mumkin. Bu registrlarga 16 lik sanoq sistemasida quyidagi boshlang‘ich qiymatlar beriladi:

A=0x67452301,

B=0xEFCDAB89,

C=0x98BADCFE,

D=0x10325476,

Ye=0xC3D2E1F0.

Keyinchalik bu o‘zgaruvchilar mos ravishda yangi *a*, *b*, *c*, *d* va *e* o‘zgaruvchilarga yozib olinadi.

*4- bosqich. Ma’lumotni 512 bitlik bloklarga ajratib qayta ishlash.*

Bu xesh funksiyaning asosiy sikli quyidagicha bo‘ladi:

for (*t* = 0; *t* < 80; *t*++){

*temp* = (*a* <<< 5) + *ft*(*b*, *c*, *d*) + *e* + W*t* + K*t* ;

*e* = *d*; *d* = *c*; *c* = *b* <<< 30; *b* = *a*; *a* = *temp*; },

Bu yerda <<< - chapga siklik surish amali. K*t* lar 16 lik sanoq sistemasida yozilgan quyidagi sonlardan iborat:

****

ft(x, y, z) funksiyalar esa quyidagi ifodalar bilan aniqlanadi:



*Wt* lar kengaytirilgan ma’lumotning512bitlik blokining32bitlik qismbloklaridan quyidagi qoida bo‘yicha hosil qilinadi:

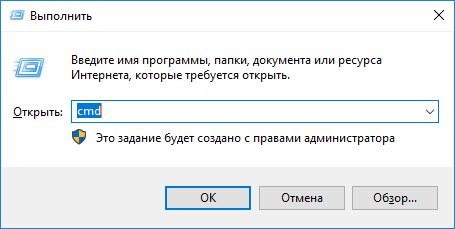


Asosiy sikl tugagandan keyin *a*, *b*, *c*, *d* va *e* larning qiymatlari mos ravishda A, B, C, D va E registrlardagi qiymatlarga qo‘shiladi hamda shu registrlarga yozib qo‘yiladi va kengaytirilgan ma’lumotning keyingi 512 bitlik blokini qayta ishlashga o‘tiladi.

*5- bosqich. Natija.*

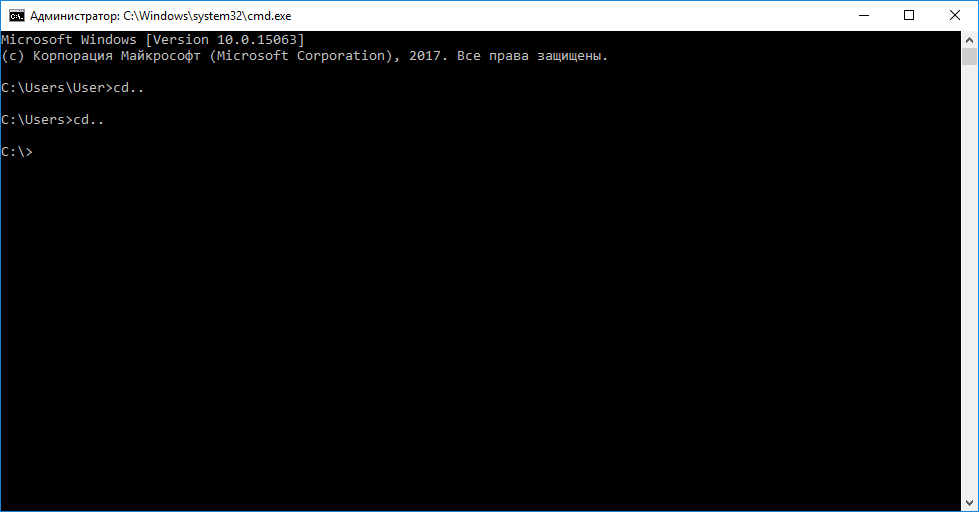
Ma’lumotning xesh qiymati A, B, C, D va Ye registrlardagi qiymatlarni birlashtirish natijasida hosil qilinadi.

**Amaliy qism**

Openssl kutubxonasidan foydalanish uchun *cmd* buyrug‘idan foydalaniladi (pusk va R teng bosiladi):

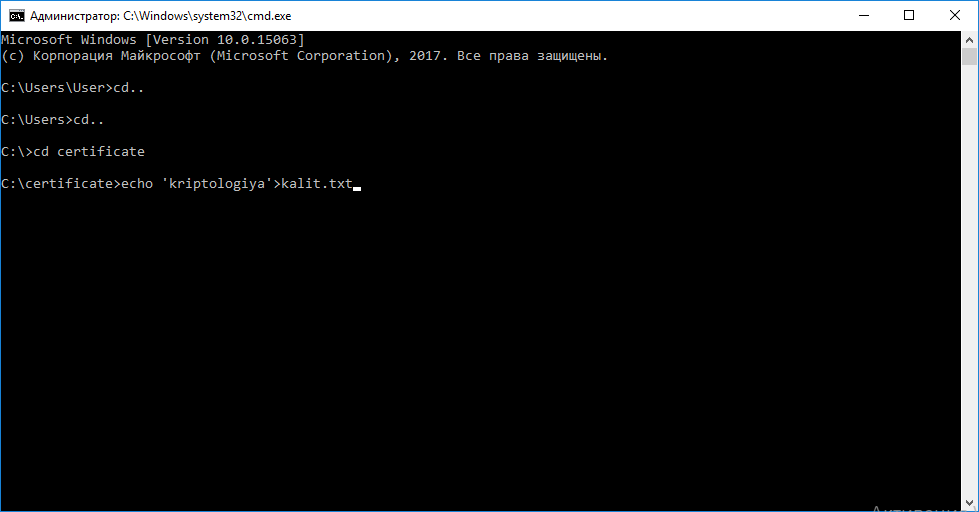
14.3- rasm. Cmd buyrug‘ini ishga tushiriladi

## Cmd oynasidagi joriy papkasidan chiqish uchun *cd..* buyrug‘idan foydalaniladi:

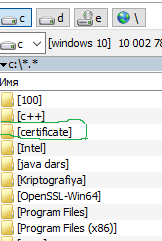


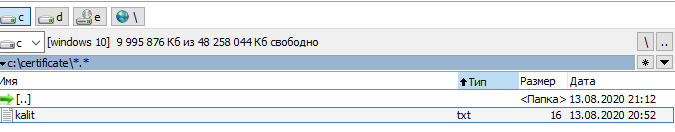
14.4- rasm. *cd..* buyrug‘idan foydalanish

Openssl kutubxonasi uchun foydalanadigan *certificate* papkasiga quyidagi buyrug’ orqali ochiq ma’lumotni xosil qilib olamiz:

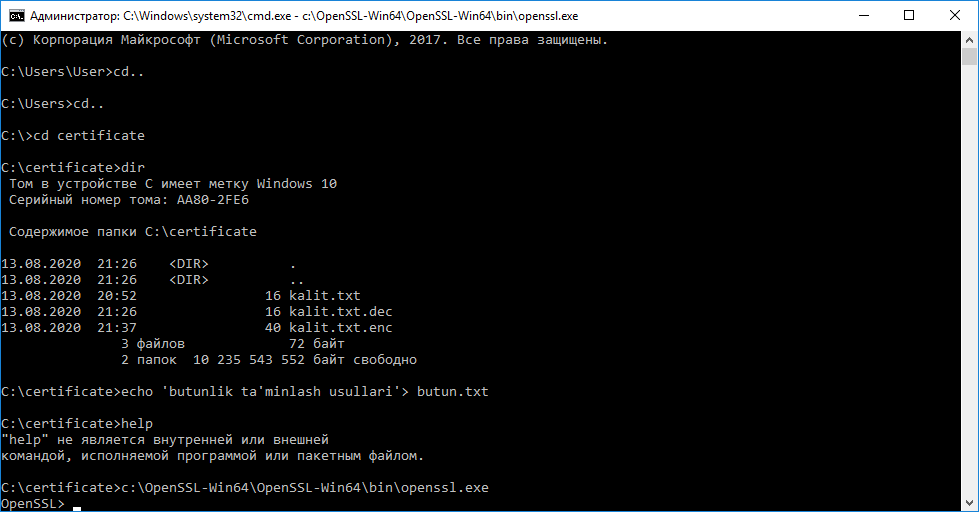


14.5- rasm. Ochiq ma’lumot ko’rsatiladi

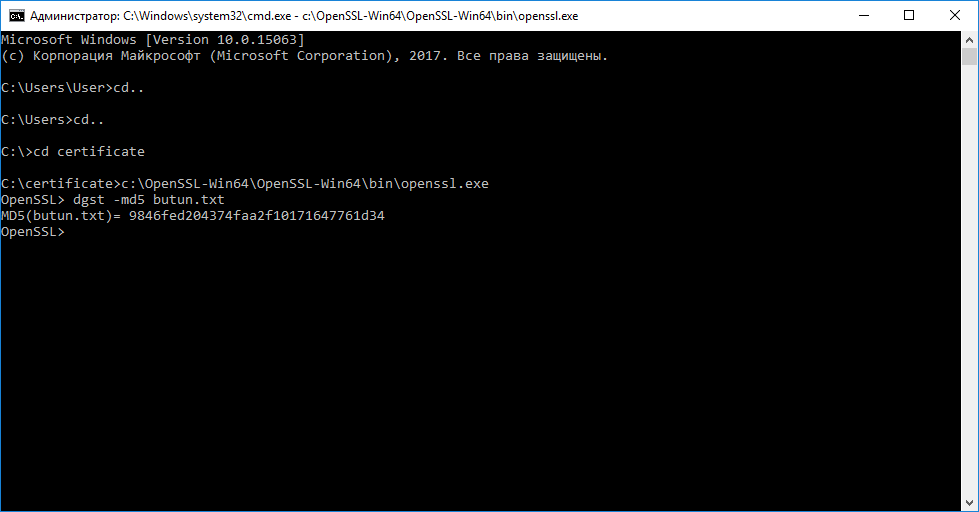
****

****

14.6- rasm. Ochiq ma’lumot joylashuvi



14.7- rasm. Opensslni ishga tushirish



14.8- rasm. Opensslda md5

**Topshiriq**

Asosiy matn xesh algoritmlaridan foydalangan holda matni butunligi ta’minlansin va qadamma – qadam izohlansin. Shuningdek *Openssl kutibxonasidan foydalangan holda* matni xesh qiymatini olish amalga oshirilsin.

**Nazorat savollari**

1. Xesh funksiyalar va ularning vazifasi nimadan iborat.
2. MD5 xesh funksiyasini tavfsiflang.
3. SHA1 xesh funksiyasida foydalanilgan matematik amallarni keltiring.

**15-Amaliy ish**

**Mavzu: Xesh qiymatlarni kalitlarni to‘liq tanlash usuli bo‘yicha aniqlash**

**Ishdan maqsad**: Xesh qiymatlarni kalitlarni to‘liq tanlash usuli bo‘yicha bilim va ko’nikmalariga ega bo‘lish.

**Nazariy qism**

To‘liq tanlash, yaʼni kalitlarning barcha mumkin bo‘lgan variantlarini tanlash usuli, kriptotaxlilchining nosimmetrik kriptotizim algoritmini va oshkora kalitni bilgan xolda barcha mumkin bo‘lgan kalitlarni tanlash va sinab ko‘rishga asoslanadi. Simmetrik kriptotizimlarda ham shifrmatn va ochiq matn asosida tuliq tanlash usuli qo‘llaniladi. Kriptotaxlilchilar ko‘pincha kompyuter yordamida kalitlarni to‘liq tanlash usulidan foydalanib shifrlarni oshkor etadilar. Kriptotaxlil jarayonida milliard kalitlarni sekundiga minglab kalit tezlikda tanlashga to‘g‘ri keladi.

Faraz qilinsin, buzg‘inchi uchun bir yoki bir necha (x, y) juftlik maʼlum bo‘lsin. Osonlik uchun xar qanday juftlik (x, y) uchun Ek(x)=y munosabatni qanoatlantiruvchi yagona k kalit mavjud bo‘lsin. Mumkin bo‘lgan kalitlar to‘plamini tartibga solinadi va K dagi kalitlarni ketma-ket ravishda Ek(x) =y tenglik bajarilishiga tekshirib chiqiladi. Agar kK kalitning bir variantini tekshirish bir amal yordamida hisoblansa, unda kalitlarni to‘liq tanlash uchun |K| amal talab etiladi. Bunda |K| - to‘plamdagi elementlar soni. Shifrlash sxemasida kalit tasodifiy va teng extimollik bilan K to‘plamdan tanlangan bo‘lsin. Bunda kalit 1/|K| extimollik bilan bilan topiladi va to‘liq tanlash usulining ish xajmi 1 ga teng bo‘ladi.

Misol uchun shaxsiy kalit uzunligi 100 bit bo‘lsa, unda barcha shaxsiy kalitlar soni 2100 ga teng, yaʼni kalitlar to‘plami quvvati |K| =2100. Shaxsiy kalit uzunligi 56 bit bo‘lganda, barcha mumkin bo‘lgan shaxsiy kalitlar soni |K| =2560.51017 ga teng. Bunda, agar hisoblash qurilmasi xar bitta maxfiy kalitga mos oshkora kalitni hisoblash va uni xech qiyinchiliksiz taqqoslash uchun 10-6 sekund vaqt sarflasa, 24 soatda barcha kalitlarni sinab chiqish uchun 5.787\*105 ta EXM kerak bo‘ladi.

Shuning uchun xam shaxsiy va shifrlashda foydalaniladigan kalitni topishni murakkablashtirish maqsadida shaxsiy kalitlar uzunligi 127-159 bitdan katta bo‘lgan uzunlikda generatsiyalanadi.

Kalitlarni to‘liq tanlash usulida sarflangan vaqt foydalanilgan kompyuter imkoniyati va kalit uzunligiga bog‘liq.

quyida keltirilgan jadvalda turli uzunlikdagi parollarni (ular turli 36 ta belgidan iborat bo‘lishi mumkin) sekundiga 100 000 parolni hisoblash imkoniga ega kompyuterda xosil qilish vaqtlari keltirilga

15.1-jadval

Kalitlarni to‘liq tanlash usuli

|  |  |  |  |
| --- | --- | --- | --- |
| Belgilar soni | Variantlar soni | Bardoshligi | Vaqti |
| 1 | 36 | 5 bit | Sekundan kam |
| 2 | 1296 | 10 bit | Sekundan kam |
| 3 | 46 656 | 15 bit | Sekundan kam |
| 4 | 1 679 616 | 21 bit | 17 sekund |
| 5 | 60 466 176 | 26 bit | 10 minut |
| 6 | 2 176 782 336 | 31 bit | 6 soat |
| 7 | 78 364 164 096 | 36 bit | 9 kun |
| 8 | 2,821 109 9x1012 | 41 bit | 11 oy |
| 9 | 1,015 599 5x1014 | 46 bit | 32 yil |
| 10 | 3,656 158 4x1015 | 52 bit | 1 162 yil |
| 11 | 1,316 217 0x1017 | 58 bit | 41 823 yil |
| 12 | 4,738 381 3x1018 | 62 bit | 1 505 615 yuz yil |

Parollarni yoki kalitlarni to‘liq tanlash usuli asosida topishda turli dasturiy vositalar foydalaniladi. Quyida parollarni aniqlashda foydalaniladigan **Rainbowcrack** dasturi haqida to‘xtalib o‘tilgan.

Ma’lumki parollar bazada saqlanishda uning o‘zi emas, balki uning xesh qiymati saqlanadi. Ushbu xesh qiymatni qaysi ma’lumotga tegishli ekanligi aniqlashda ushbu dasturiy ta’minotdan foydalaniladi. Ushbu dasturiy ta’minotdan foydalanish uchun quyidagi ketma – ketliklarni bajarish talab etiladi.

* 1. Rainbowcrack dasturiy vositasini ko’chirib olinadi. Uning hozirgi kundagi oxirgi versiyasi *rainbowcrack-1.6.1.*
  2. Ushbu dasturiy vositadan foydalanishda jadvallar (ko‘p xesh qiymatlardan iborat bo‘lgan) zarur bo‘ladi. Ushbu jadvallar turli alifbolar uchun mavjud (alifbodagi belgilarning soniga va tarkibiga ko‘ra jadvallar ko‘p bo‘lishi mumkin). Bu alifbolarni dasturiy vositaning veb sahifasi orqali ko’chirib olish mumkin yoki foydalanuvchini o’zi hosil qilish mumkin. Alifbolarga misol qilib quyidagilarni keltirish mumkin:

numeric = [0123456789]

alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]

alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]

loweralpha = [abcdefghijklmnopqrstuvwxyz]

loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]

mixalpha = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ] mixalpha-numeric =

[abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]

ascii-32-95=[!"#$%&'()\*+,-

./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_`abcdefghijklmnopqrstuvwxyz{|}~]

ascii-32-65-123-4=[!"#$%&'()\*+, ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_`{|}~]

alpha-numeric-symbol32-space=

[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&\*()-\_+=~`[]{}|\:;"'<>,.?/ ]

* 1. Ushbu labaratoriya ishida ikkinchi usulda foydalanilgan holda jadvallarni hosil qilish ko‘rib chiqiladi. Buning uchun kiritilgan parolning uzunligi (minmal va maksimal, oraliqda) va qaysi alifbodan foydalanganligi qanchalik ma’lum bo‘lsa, ushbu dasturdan natija olish shuncha aniq bo‘ladi. Ushbu labaratoriya ishida alifbo sifatida “abcdef” ni va parol uzunligini 4 ga teng deb olingan hol uchun qaraladi. Alifbo va parolning uzunligini ortishi hisoblash vaqtini ko‘p talab qiladi. Bundan tashqari parollarni xesh qiymatlarini hisoblashda foydalanilgan xesh funksiyasini bilish talab etiladi.
  2. Dasturiy vosita ichidagi “charset.txt” deb nomlangan faylga yangi kiritilgan alifba “custom = [abcdef]” tarzida yoziladi va *rcrack.exe* dasturi ishga tushiriladi. Ushbu dastur buyruqlar oynasida ishlagani bois, undagi buyruqlar quyidagilardan iborat.

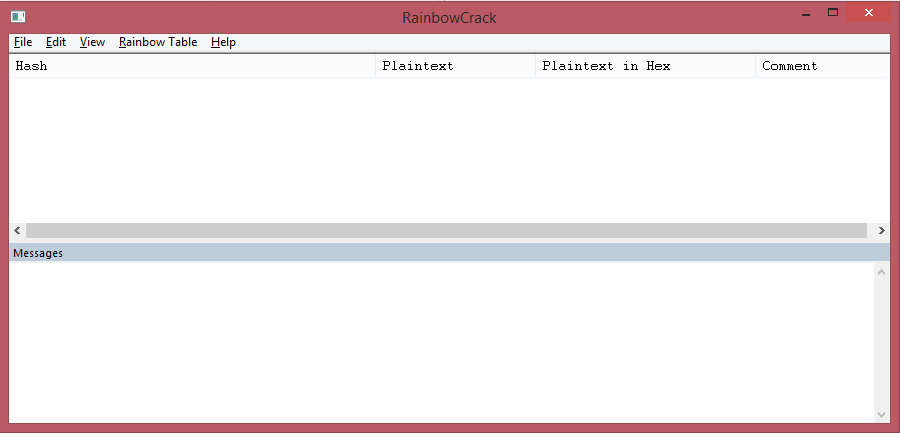
- rtgen hash\_algorithm charset plaintext\_len\_min plaintext\_len\_max table\_index chain\_len chain\_num part\_index

15.2- jadval

Har bir buyruqning manosi

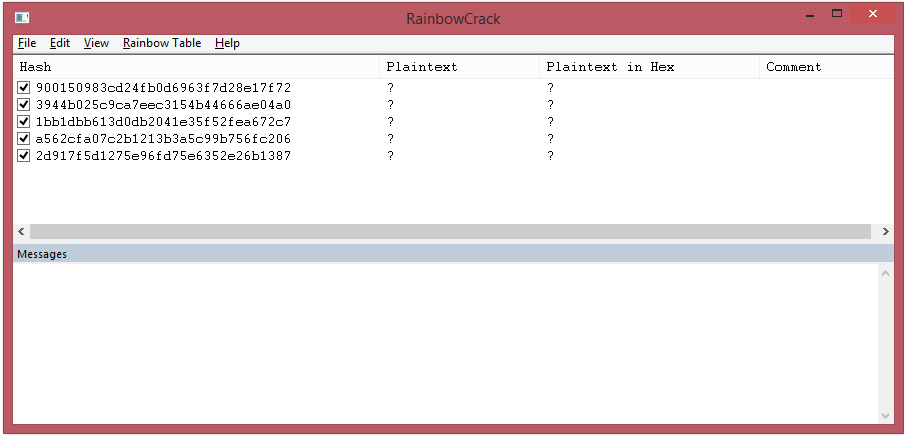
|  |  |
| --- | --- |
| hash\_algorithm | Xesh algoritmining nomi |
| charset | Alifboning nomi |
| plaintext\_len\_min  plaintext\_len\_max | Parollarning minimal va maksimal uzunliklari |
| table\_index | Bu parametr kamaytirish funksiyasini tanlash uchun  foydalaniladi. |
| chain\_len | Kattaliklarni saqlash uchun xotira yacheykasi o‘lchami.  Katta o‘lchamli xotira ko‘p uzunlikdagi parollar uchun. |
| chain\_num | Yacheykalar soni. |
| part\_index | Katta jadvalni saqlashda kichik fayllarda saqlashda  ular bo’linadi. Bu parmetr ularni tanish uchun ishlatiladi. |

* 1. Yuqoridagi buyruqlar oynasidan foydalanilgan holda, aytilgan hol uchun : *rtgen md5 custom 1 4 2400 100000 all* buyruq hosil qilindi.
  2. Yuqoridagi buyruq amalga oshirilgandan so‘ng, joriy katalogda “md5\_custom#1-4\_0\_2400x100000\_0.rt” nomli jadval hosil bo‘ladi.
  3. Ushbu jadvaldan foydalanish uchun “rcrack\_gui.exe” qism dastur ishga tushiriladi. Uning ko‘rinishi quyidagicha:



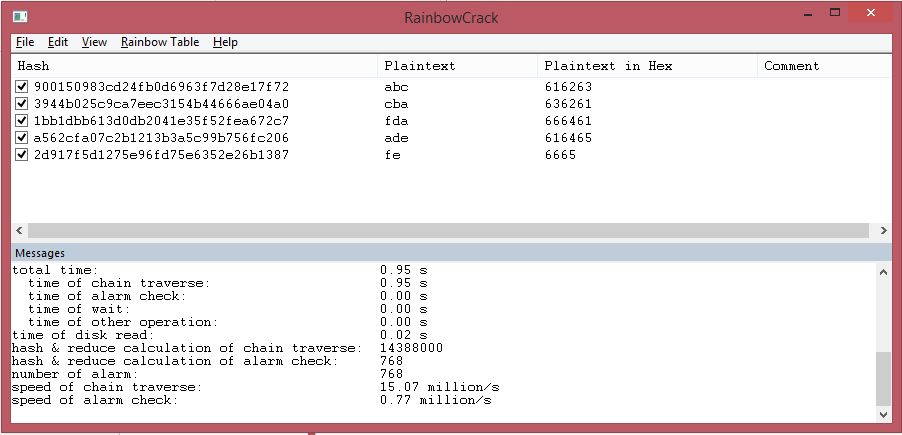
15.1– rasm. Dasturning umumiy ko‘rinishi

* 1. Ushbu dasturdan foydalanish uchun, dastlab paroli aniqlanadigan xesh qiymatlar olinadi va dasturning “*Files/Add Hashes…*” bandiga kiritiladi. Masalan, quyidagi xesh qiymatlar kiritilsin:



15.2– rasm. Xesh qiymatlarni hisoblash

* 1. Xesh qiymatlarga mos parolni aniqlash uchun hosil qilingan jadvalni “*Rainbow Table/Search Rainbow Tables…*” bandi orqali kiritiladi. Shundan so‘ng dastur tomonidan xesh qiymatlarga mos bo‘lgan parol dastur tomonidan aniqlanadi. Agar parol aniqlansa, “Plaintext” ustinida yoziladi. Aks holda “???” belgisi hosil bo‘ladi. Yuqoridagi hol uchun olingan natijalar quyidagicha:



15.3– rasm. Xesh qiymatlarni aniqlash

* 1. Odatda tezroq qidirish maqsadida hosil bo‘lgan tartiblash amalga oshiriladi. Ushbu vazifa “*rtsort*” dastur orqali amalga oshiriladi. Masalan, quyidagi buyruqni kiritish orqali mavjud katalogdagi barcha jadvallarni tartiblash mumkin: “rtsort \*.rt”.

**Topshiriq**

Har bir talaba o’ziga biriktirilgan xesh qiymatlarga mos ochiq matnni yoki parolni aniqlasin. *Izoh:* bu yerda MD5 xesh funksiyasi va “*loweralpha = [abcdefghijklmnopqrstuvwxyz]*” alifbodan foydalanilgan. Ochiq matnlar yoki parollarning maksimal uzunligi 6 ga teng.

|  |  |  |
| --- | --- | --- |
| **№** | **Xesh qiymat** | **Javob** |
| 1. | f97c5d29941bfb1b2fdab0874906ab82 |  |
| 2. | c4988dbf8716d62d17180dd114f15c71 |  |
| 3. | 66058ec26cd62e957604145e726b0f0b |  |
| 4. | b8a9f715dbb64fd5c56e7783c6820a61 |  |
| 5. | 35d6d33467aae9a2e3dccb4b6b027878 |  |
| 6. | 7f46165474d11ee5836777d85df2cdab |  |
| 7. | 0800fc577294c34e0b28ad2839435945 |  |
| 8. | 7f5f2244206f1ebac53dc0a333176b68 |  |
| 9. | aa2d6e4f578eb0cfaba23beef76c2194 |  |
| 10. | 755f85c2723bb39381c7379a604160d8 |  |
| 11. | bae60998ffe4923b131e3d6e4c19993e |  |
| 12. | 7eeeb0fbb2f55bd9a94681488f0c75de |  |
| 13. | 4af3318a57ca352daaac11aa778ff083 |  |
| 14. | 341be97d9aff90c9978347f66f945b77 |  |
| 15. | 639bae9ac6b3e1a84cebb7b403297b79 |  |
| 16. | ab86a1e1ef70dff97959067b723c5c24 |  |
| 17. | 0d149b90e7394297301c90191ae775f0 |  |
| 18. | d850f04cdb48312a9be171e214c0b4ee |  |
| 19. | 6057f13c496ecf7fd777ceb9e79ae285 |  |
| 20. | 444bcb3a3fcf8389296c49467f27e1d6 |  |
| 21. | 1a1dc91c907325c69271ddf0c944bc72 |  |
| 22. | c47d187067c6cf953245f128b5fde62a |  |
| 23. | 63a9f0ea7bb98050796b649e85481845 |  |
| 24. | 98bd1c45684cf587ac2347a92dd7bb51 |  |

## Nazorat savollari

1. Kalitlarni to‘liq tanlash usulining afzalliklari va kamchiliklarini keltiring.
2. Ushbu tahdiddan himoyalanish uchun qanday amallarni bajarish kerak.