O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI URGANCH FILIALI

DAVLANOV UMARBEK MADAMINOVICH

AXBOROT TIZIMLARIDA AXBOROTLARNI KRIPTOGRAFIYA ALGORITIMLAR ASOSIDA XIMOYALASH

mavzusida

REFERAT

Urganch – 2017 y.

MUNDARIJA

KIRISH

1. Java dasturlsh tili imkoniyatlari

2. JDK ni yuklab olish va o’rnatish

3.“Axborot tizmida axborotlarni kiptografiya algoritmlari asosida himoyalash dasturi” ni loyihalash

5.Foydalanuvchi uchun yo’riqnoma

FOYDALANILGAN ADABIYOTLAR

KIRISH

XX asr oxirida “axboriy jamiyat” va “axborotlashuv” atamalari nafaqat mazkur soha vakillari, balki siyosatchilar, iqtisodchilar, olimlar va pedagoglar lug’at boyligidan ham mustahkam o'rin egalladi. Ko'p hollarda bu tushuncha fuqarolik jamiyati platformasida yangi evolyutsion odimni amalga oshirib XXI asrga axborotlashgan jamiyat sifatida munosib kirib borish imkonini beradigan axborot - kommunikatsiya texnologiyalari, telekommunikatsiya vositalarining rivojlanishi bilan uyg’un holda ta'riflanadi. Dunyo yangi davr-axborot asriga, elektron iqtisodiy faoliyat, tarmoq jamoatlari va chegarasiz tashkilotlar asriga qadam qo'ydi. Yangi davrning boshlanishi jamiyat hayotining iqtisodiy va ijtimoiy tomonlarini tubdan o'zgartirishi tabiiy. Bunday o'zgarishlar informatsion dunyodagi inson roliga bevosita ta'sir ko'rsatadi. Boisi inson jamiyatning axboriy-texnik xususiyatlari yo'nalishiga mos ravishda o'zgarib boradi.

1. Java dasturlsh tili imkoniyatlari

Java universal obyektga yo’naltirilgan dasturlash tili bo’lib, uning imkoniyatlari juda katta. 1995- yilda Sun Microsystems kompaniyasi tamonidan ishlab chiqilgan. Birinchi afzallik tamoni unda yaratilgan dasturiy ta’minot har qanday Operatsion tizimda muommosiz ishlaydi. Java dasturlash tili C, C++, Eiffel, SmallTalk, Objective C и Cedar/Mes kabi eng yaxshi dasturlash tillari konsepsiyali asosida yaratilgan. Demak Java bu dasturlash tillarida yechiladigan masalalarning barchasini yecha oladi. Masalan C++ dasturlash tilida komanda satri utilitalarini yaratish imkoniyati va boshqa dasturlarning CUI – ilovalarini yaratish imkoniyatlari mavjud. Bu jihatdan Java bu dasturlash tillaridan farq qilmaydi. Quyida Java yordamida yaratish mumkin bo’lgan ilovalar berilgan:

- Apletlar(mini ilovalat)
- CUI ilovalar
- Komanda satri uchin ilovalar
- Paketlar(kutibxonalar)

Javada yaratilgan dastur xafsizlik imkoniyati katta. Shuning uchun tarmoqda ishlovchi dasturlar ko'pchiligi Javada yaratilmoqda.Bularga mobil dasturlar, o'yinlar, web serverlar va koorparativ dasturiy ta'minotlarni misol qilish mumkin.

Butun dunyo bo'yicha 9 milliondan ortiq mutaxasis Java tilida dastur tuzishadi.

Ixcham kompyuterlardan tortib ma'lumotlarni to'plash markazlarigacha, o'yin konsollaridan tortib super kompyuterlargacha, uyali telefonlardan tortib internet tarmog'igacha, barcha-barchasida Javadan foydalaniladi.

- Java 1.1 mlrd. dan ortiq shaxsiy kompyuterlarda ishlatiladi
- Har yili 930 million Java dasturiy ta'minotlari registratsiya qilinadi
- Java 3 mlrd. mobil telefon vositalarida ishlatiladi
- Har yili Java telefonlari Apple va Android telefonlaridan 31 marta ko'p sotiladi
- Har yili 1.4 mlrd. Java Card platformasi ishlab chiqiladi
- Java texnologiyasi asosida televizion qo'shimcha qurilmalar, printerlar, o'yinlar, avtomobil navigatsiya tizimlari, bankomatlar, lotareya terminallari, meditsina asboblari, avtamotik to'lov tizimlari va boshqa ko'plam qurilmalar ishlab chiqiladi.

Java tilida yaratilgan dastur ishlashi uchun uning dastlab komplyatorini o'rnatish kerak. Bu komplyator JDK(Java Development Kit) bo'lib, u dasturni bajarib beradi. JDK ning bugungi kunda qo'llaniladigan versiyalari jdk-1.6 va jdk-1.7 versiyalari bo'lib eng ohirgi versiyasi 1.7.

2.2.JDK ni yuklab olish va o'rnatish.

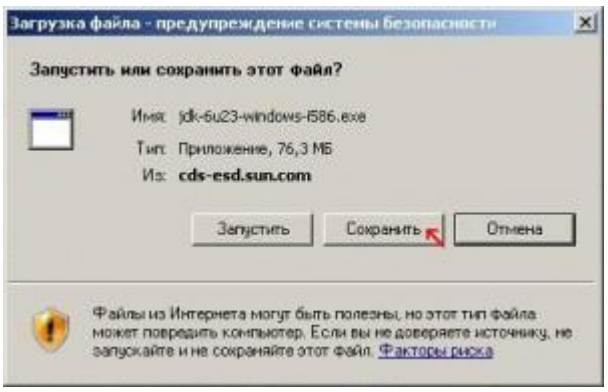
JDK ni http://www.oracle.com/technetwork/java/javase/downloads/index.html sayti orali yuklab olish mumkin.

U yerdan qaysi platform uchun yuklashimizni tanlaymiz

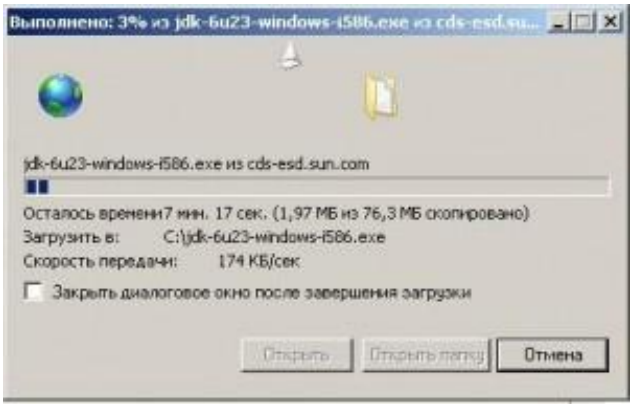
Shartga rozilikni bildiramiz

va faylni yuklaymiz.

Vaylni saqlaymiz.

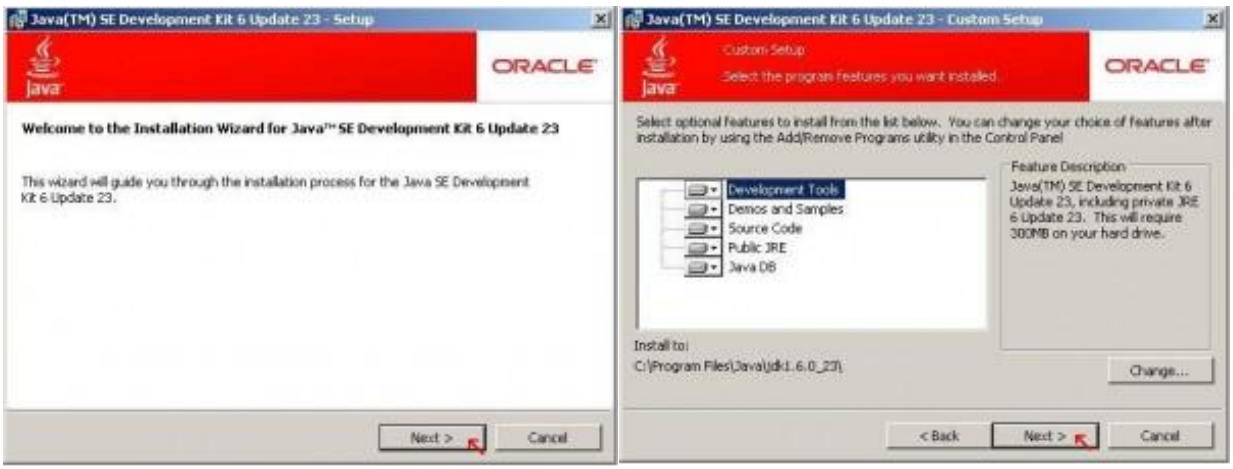


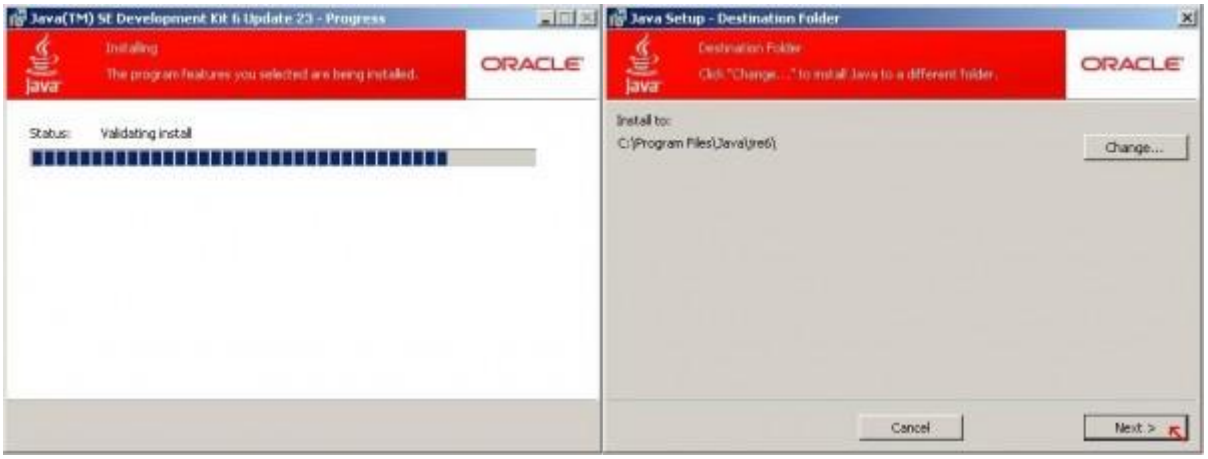
Yuklab olishini kutib yuramiz.



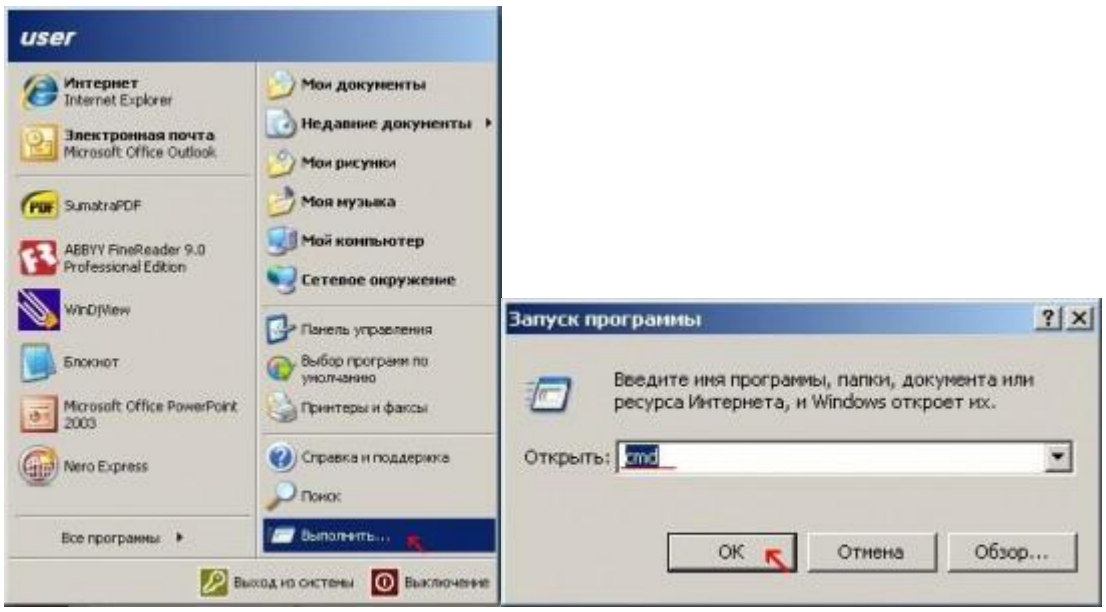
JDK ni o’rnatish

Faylni yuklab bo’lgandan so’ng uni o’rnatishga o’tamiz. Bunda hech qanday qiyinchilik yo’q faqatgina Next tugmasini bosishdan iborat.



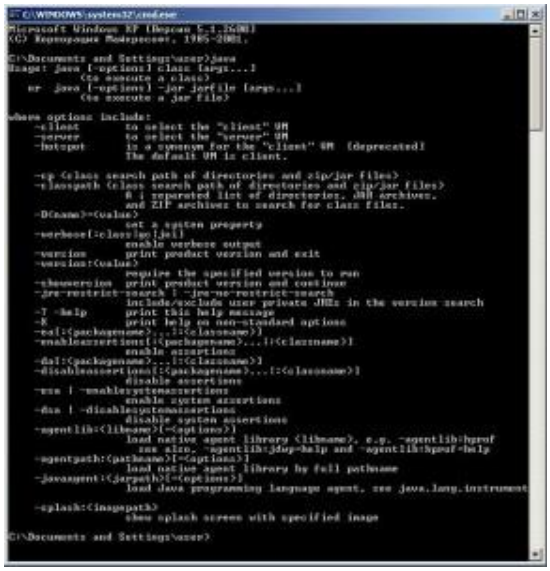


Endi uning qanday o’rnatilganligini tekshiramiz. Uning uchun komanda satrini ochamiz.

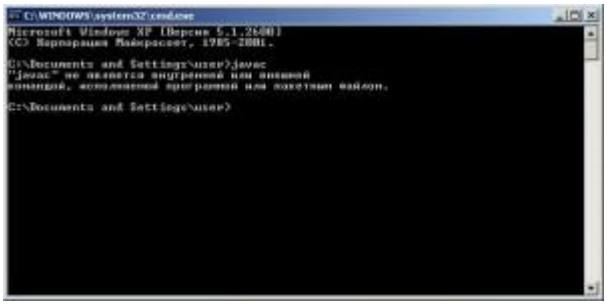


va undan Java buyrug’ini ishga tushirishga harakat qilamiz

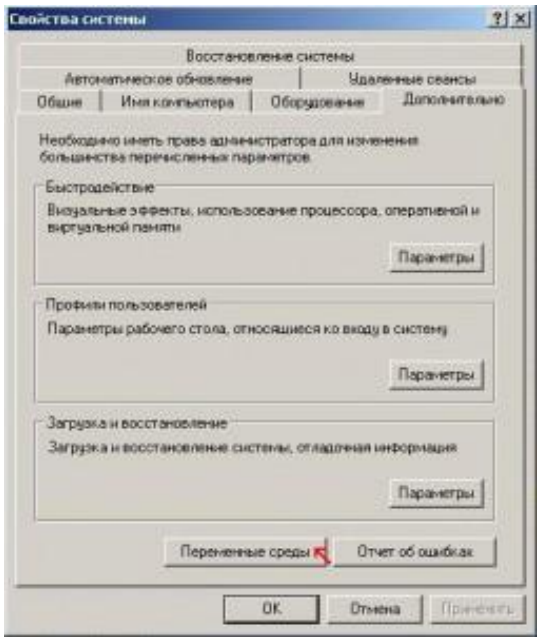
.



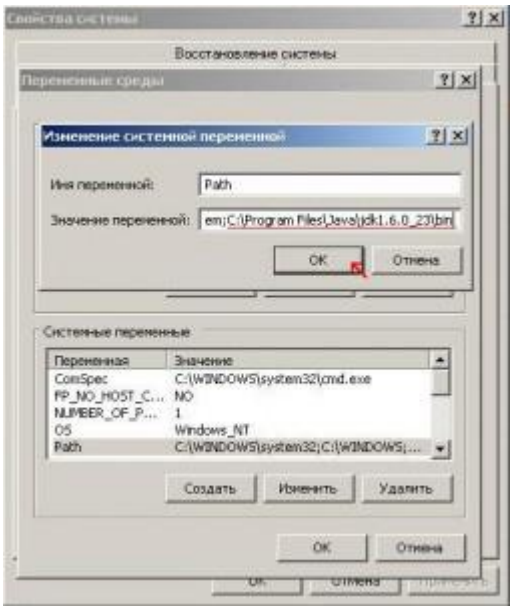
Agar unda ishga tushirish bo’yicha yo’riqnomani ko’rsak u holda hech narsa qilish shart emas. Lekin agar konsolda “не является внутренней или внешней командой” yozuvini ko’rsak



U holda PATH o’zgaruvchisida unga yo’lni ko’rsatib yuborish kerak. Buni bajarish juda oson. “Мой компьютер” ning свойства sini ochamiz va undan “Переменные среды” tugmasini bosamiz.



va JDK ga bo’lgan yo’lni ko’rsatamiz.



endi hammasi joyda bo’ladi.

3.“Axborot tizmida axborotlarni kiptografiya algoritmlari asosida himoyalash dasturi” ni loyihalash.

“Axborot tizmida axborotlarni kiptografiya algoritmlari asosida himoyalash dasturi” ni loyihalashda asosan shifrlash algaritmlariga e’tibor qaratishimiz lozim. Bu dastur orqali biz kompyuter muhitida har qanday ma’lumotni himoyalay olishimiz kerak. Kiptografik usulda ma’lumotni himoyalashda asosan AES, DES, SHA-256, HMAC algoritimlaridan foydalanamiz.

DES blokli shifrlash algoritmi 1999-yilgacha AQShda standart shifrlash algoritmlari sifatida ishlatib kelingan.

1974-yildan Amerika qo‘shma shtatlarining standart shifrlash algoritmi sifatida qabul qilingan DES shifrlash algoritmi quyidagi :

- kalit uzunligining kichigligi (56 bit);
- S-blok akslantirishlarining differensial kriptotahlil usuliga bardoshsizligi;

va boshqa sabablarga ko‘ra eskirgan deb sanaladi . Ayniqsa 1999 yilda DES shifrlash algoritmi yordamida shifrlangan malumotning Internet tarmog‘iga ulangan 300 ta paralel kompyuter tomonidan yigirma to‘rt soat davomida ochilishi haqidagi malumotning tasdiqlanishi bundan keyin mazkur standart algoritmi yordamida malumotlarni kriptografik muhofaza qilish masalasini qaytadan ko‘rib chiqish va yangi standart qabul qilish zaruratini keltirib chiqardi.

Amerika qo‘shma shtatlarining “Standartlar va Texnalogiyalar Milliy Instituti

(NIST)” 1997-yilda XXI asrning ma'lumotlarni kriptografik muhofazalovchi yangi shifrlash algoritmi standartini qabul qilish maqsadida tanlov e'lon qildi. 2000 yilda standart shifrlash algoritmi qilib, RIJNDAEL shifrlash algoritmi asos qilib olingan AES (Advanced Encryption Standard) (FIPS 197) qabul qilindi. Algoritmning yaratuvchilari Belgiyalik mutaxassislar Yon Demen (Joan Daemen) va Vinsent Ryumen (Vincent Rijmen)larning familiyalaridan RIJNDAEL nomi olingan .

AES FIPS 197 blokli shifrlash algoritmida 8 va 32-bitli (1-baytli va 4-baytli) vektorlar ustida amallar bajariladi. AES FIPS 197 shifrlash algoritmi XXI asrning eng barqaror shifrlash algoritmi deb hisoblanadi. Bu algoritm boshqa mavjud standart simmetrik shifrlash algoritmlaridan farqli o‘laroq, Feystel tarmog‘iga asoslanmagan blokli shifrlash algoritmlari qatoriga kiradi.

AES algoritmida baytlar ustida amallar bajariladi. Baytlar $GF(2^8)$ chekli maydon elementlari sifatida qaraladi. $GF(2^8)$ maydon elementlarini darajasi 7 dan katta bo‘lmagan ko‘phad sifatida tasvirlash mumkin. Agarda baytlar

$$\{a_7a_6a_5a_4a_3a_2a_1a_0\},\ a_i \in \{0,1\},\ i = \overline{0...7}$$

ko‘rinishda tasvirlangan bo‘lsa, u holda maydon elementlari quyidagicha ko‘phad ko‘rinishda yoziladi:

$$a_7 \cdot x^7 + a_6 \cdot x^6 + a_5 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

Misol uchun $\{11010101\}$ baytga $x^7 + x^6 + x^4 + x^2 + a_0$ ko‘rinishdagi ko‘phad mos keladi.

Chekli $GF(2^8)$ maydon elementlari uchun additivlik va multiplikativlik xossalariga ega bo‘lgan qo‘shish va ko‘paytirish amallari aniqlangan.

AES algoritmida ko‘phadlarni qo‘shish $\oplus$ **(XOR)** (berilgan ko‘phadlarga mos keluvchi ikkilik sanoq sistemasidagi sonlarni mos bitlarini mod 2 bo‘yicha qo‘shish) amali orqali bajariladi. Masalan

$x^7 + x^6 + x^4 + x^2 + x$ va $x^7 + x^5 + x^3 + x + 1$ ko‘phadlar natijasi quyidagicha hisoblanadi:

$$(x^7 + x^6 + x^4 + x^2 + x) \oplus (x^7 + x^5 + x^3 + x + 1) = (x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

Bu amal ikkilik va o‘n oltilik sanoq sistemalarida quyidagicha ifodalanadi:

$\{11010110\}_2 \oplus \{10101011\}_2 = \{01111101\}_2$ va $D6_{16} \oplus AB_{16} = 7D_{16}$

Chekli maydonda istalgan nolga teng bo‘lmagan a element uchun unga teskari bo‘lgan $-a$ element mavjud va $a+(-a)=0$ tenglik o‘rinli, bu erda nol elementi sifatida $\{00\}_{16}$ qaraladi. $GF(2^8)$ maydonda $a \oplus a = 0$ tenglik o‘rinli.

AES algoritmida ko‘phadlarni ko‘paytirish quyidagicha amalga oshiriladi:

- ikkita ko‘phad o‘nlik sanoq sistemasida ko‘paytiriladi;
- ettinchi darajadan katta bo‘lgan har qanday ko‘phadni sakkizinchi darajali $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ keltirilmaydigan ko‘phadga bo‘lganda qoldiqda etti va undan kichik bo‘lgan darajadagi ko‘phadlar hosil bo‘lib, ular natija sifatida olinadi, bunda bo‘lish jarayonida bajariladigan ayirish amali ikkilik sanoq sistemasida, yuqorida keltirilgani kabi, $\oplus$ amali asosida bajariladi.

Ana shunday qilib kiritilgan ko‘paytirish amali $\bullet$ bilan belgilanadi.

Masalan, $(x^6 + x^4 + x^2 + x + 1)$ va $(x^7 + x + 1)$ ko‘phadlar quyidagicha ko‘paytiriladi:

- bu ko‘phadlar o‘nlik sanoq sistemasida ko‘paytiriladi

$$(x^6 + x^4 + x^2 + x + 1) \bullet (x^7 + x + 1) = (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1);$$

- natija $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ keltirilmaydigan ko‘phadga bo‘linadi va qoldiq olinadi

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^7 + x^6 + 1).$$

Haqiqatan ham $(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) = (x^5 + x^3) \bullet$

$\bullet (x^8 + x^4 + x^3 + x + 1) \oplus (x^7 + x^6 + 1)$.

Har qanday nolga teng bo‘lmagan element uchun $a \bullet 1 = a$, tenglik o‘rinli. $GF(2^8)$ maydonda bir element sifatida $\{01\}_{16}$ tushiniladi.

Kiritilgan ko‘paytirish amali umumiy holda quyidagicha bajariladi. Ixtiyoriy ettinchi darajali

$$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

ko‘phadni x ga ko‘paytirib, quyidagiga ega bo‘lamiz

$$a_7x^8 + a_6x^7 + a_5x^6 + a_4x^5 + a_3x^4 + a_2x^3 + a_1x^2 + a_0x.$$

Bu ko‘phadni $\varphi(x) = x^8 + x^4 + x^3 + x + 1 = 1\{1b\}$ modul bo‘yicha hisoblab, chekli $GF(2^8)$ maydonga tegishli elementni hosil qilamiz. Buning uchun $a_7 = 1$ bo‘lganda

$\varphi(x) = x^8+x^4+x^3+x+1$ ko‘phadni yuqorida olingan sakkizinchi darajali ko‘phaddan *XOR* amali bilan ayirish kifoya, ya'ni :

$$(a_7 \oplus 1)\,x^8+(a_6 \oplus 0)\,x^7+(a_5 \oplus 0)\,x^6+(a_4 \oplus 0)\,x^5+(a_3 \oplus 1)\,x^4+(a_2 \oplus 1)\,x^3+$$
$$+(a_1 \oplus 0)x^2+(a_0 \oplus 1)\,x+1=(a_6 \oplus 0)\,x^7+(a_5 \oplus 0)\,x^6+(a_4 \oplus 0)\,x^5+$$
$$+(a_3 \oplus 1)\,x^4+(a_2 \oplus 1)\,x^3+(a_1 \oplus 0)x^2+(a_0 \oplus 1)\,x+1,$$

bu erda $a_7=1$ bo‘lgani uchun

$$(a_7 \oplus 1)\,x^8=(1 \oplus 1)\,x^8=0.$$

Agarda $a_7=0$ bo‘lsa, u holda natija: $a_6 x^7+\ldots+a_1x^2+a_0x$ ko‘phadning o‘zi bo‘ladi.

Ushbu *x time* ( ) funksiya yuqorida kiritilgan ko‘paytirish amaliga nisbatan berilgan ko‘phadni *x* ga ko‘paytirishni ifodalasin. Shu funksiyani *n* marta qo‘llab x^n ga ko‘paytirish amali aniqlanadi. Bevosita hisoblash bilan quyidagilarni o‘rinli ekanligiga ishonch hosil qilish mumkin:

$$\{57\}\bullet\{13\}=\{fe\},$$

chunki

$$\{57\}\bullet\{02\}=x\ time\ (\{57\})=\{ae\}$$
$$\{57\}\bullet\{04\}=x\ time\ (\{ae\})=\{47\}$$
$$\{57\}\bullet\{08\}=x\ time\ (\{47\})=\{8e\}$$
$$\{57\}\bullet\{10\}=x\ time\ (\{8e\})=\{07\},$$

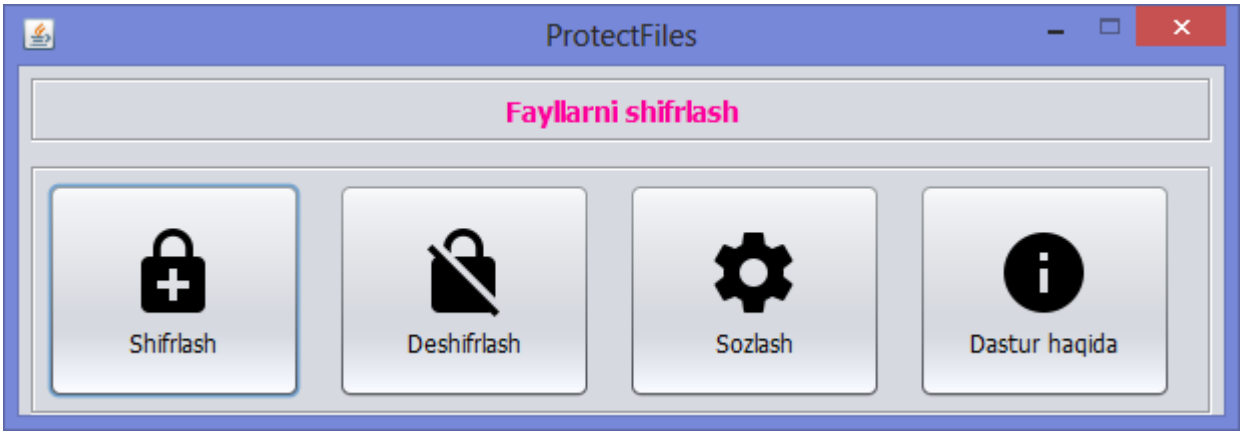
Bundan

$$\{57\}\bullet\{13\}=\{57\}\bullet(\{01\}\oplus\{02\}\oplus\{10\})=\{57\}\oplus\{ae\}\oplus\{07\}=\{fe\}.$$

5.Foydalanuvchi uchun yo’riqnoma.

Ushbu “Axborot tizmida axborotlarni kripografiya algoritmlari asosida himoyalsh” dasturimiz Java tili tuzilgan bo’lib, har xil turdagi elektron ma’lumotlarni himoyash uchun foydalaniladi. Bu dasturni ishlatishimiz uchun avvalo bor bizning o’rnatmoqchi bo’lgan kompyuterimizga java tilini taniy oladigan dasturni o’rnatishimiz kerak, ya’ni “jdk” faylni.

Shundan keyin biz dasturimizni o’rnatamiz va quydagicha oyna hosil bo’ladi:



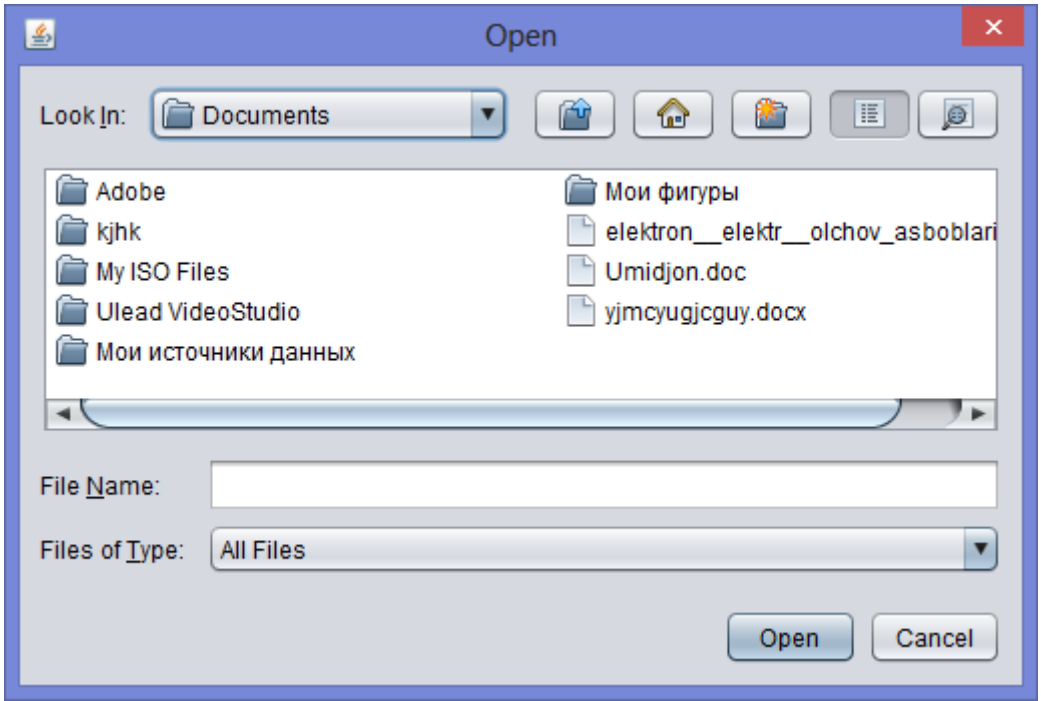
2.5-1-rasm. “Axborot tizmida axborotlarni kripografiya algoritmlari asosida himoyalsh” dasturining bosh menusi.

Bu biz yaratgan dasturimizning asosiy menusi hisoblanadi.

Bunda ko’rib turganingizdek “shifrlash”, “deshifrlash”, “sozlashlar”, “dastur haqida” deb ko’rsatilgan bo’limlardan iboratdir.

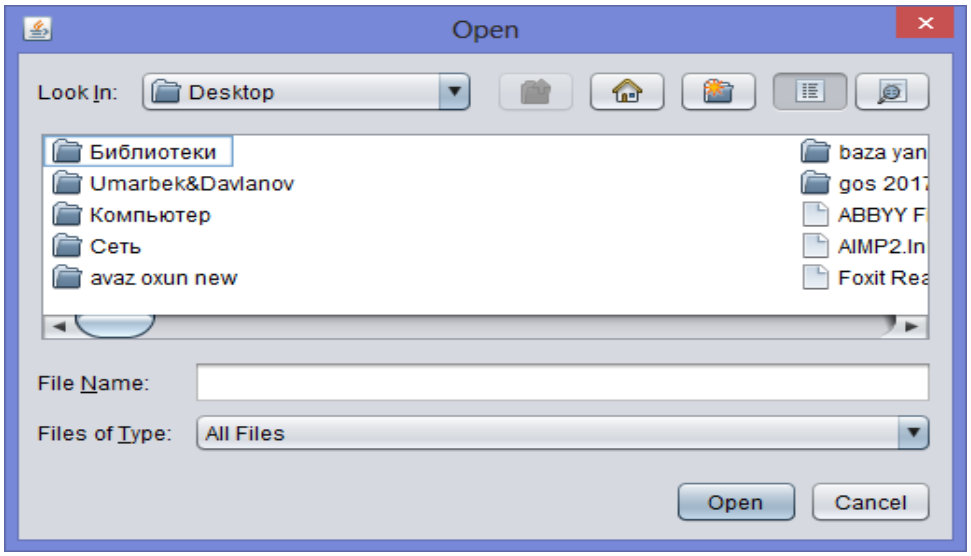
Dastlab ishlatib ko’rishni “shifrlash” bo’limidan boshlaymiz va unga to’liqligicha izoh berib o’tamiz. “shifrlash” bo’limida himoyalanishi kerak bo’lgan ma’lumotlar yoki ma’lumot kripdografiya usulidan foydalangan holda shifrlanadi. Bu dasturda biz har xil turdagi ma’lumotni himoyalashimiz mumkin. Masalan **doc, exe, mp3, mp4, pdf, ppt** va boshqa turdagi ma’lumotlarni himoyalashimiz mumkin.

“shifrlash” bo’limini ishga tushirish uchun sichqonchamiz chap tugmasini ikki marta bosamiz yoki klaveturamizdan **Ctrl+E** tugmalarini bosamiz va quydagicha oyna hosil bo’ladi:



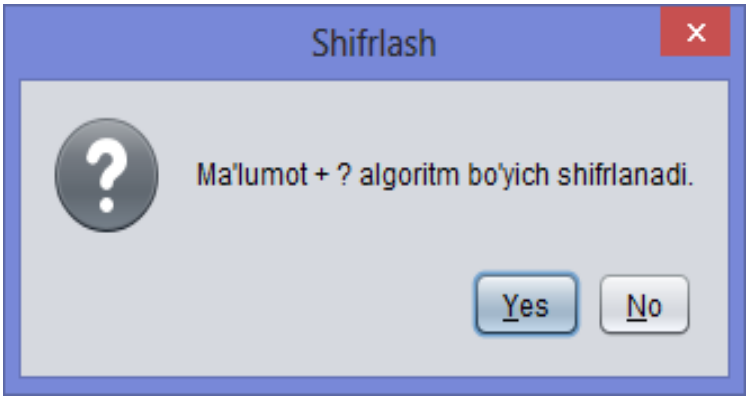
2.5-2-rasm.Shifrlash bo’limini ishga tushirish.

Bu oyna orqali biz himoyalamoqchi bo’lgan ma’lumot joyshgan joyni ko’rsatamiz. Masalan **ish stolidagi** biron bir ma’lumotni himoyalaymiz. Buning uchun biz oynadagi **look in** ga kirib ish stolini(desktop) tanlaymiz:



2.5-3-rasm.Shifrlash bo’limini ishga tushirish.

Shu joydan ma’lumotni tanlaymiz va **open** tugmasini bosamiz:



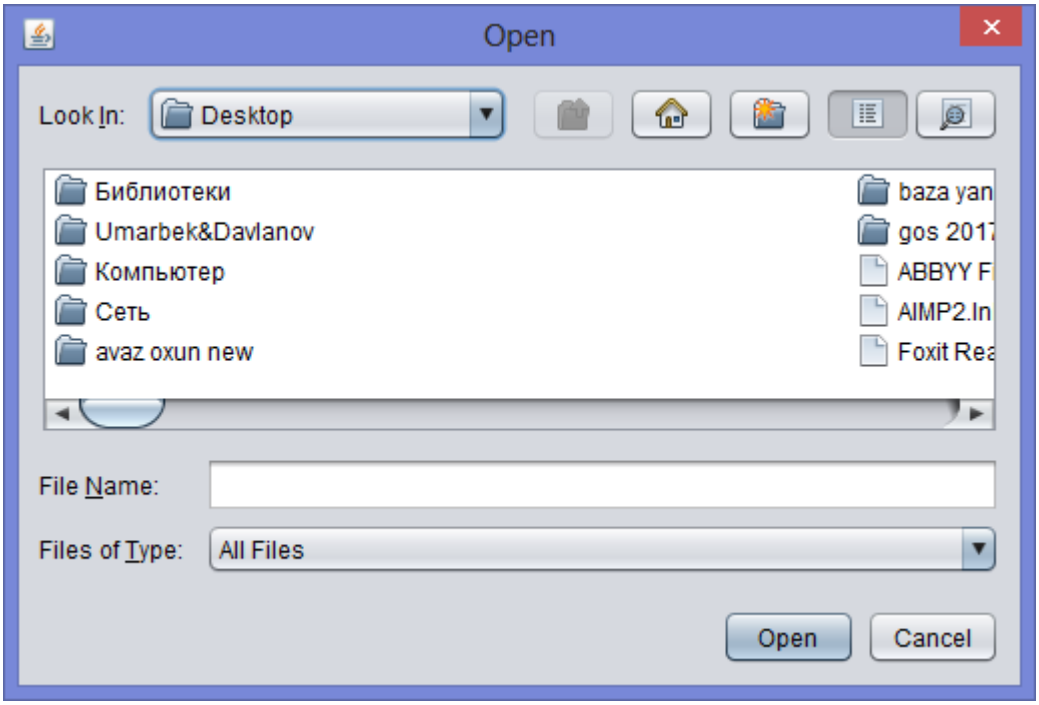
2.5-3-rasm.Ma’lumotni himoyalash haqida ogohlantirish beruvchi oyna.

Quydagicha oyna hosil bo’ladi va **yes** tugmasini bosamiz va bizga fayl shifrlanganligi haqida xabar beradi:

2.5-4-rasm.Ma’lumot himoyalanganligi haqida xabar beruvchi oyna.

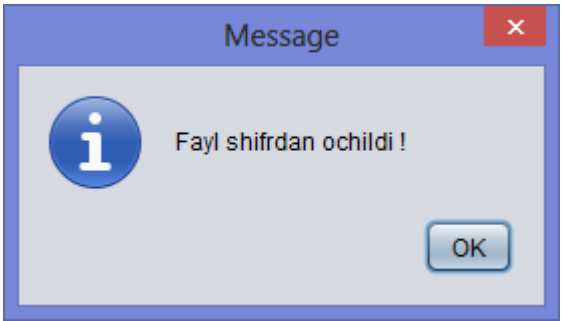
Shu tariqa ma’lumotimiz himoyalanadi va joylshgan joyida **enc** fayl sifatida ko’rsatilinib turiladi.

“deshifrlash” bo’limida biz himoyalangan ma’lumotimizni asl holiga qaytaramiz ya’ni himoyani olib tashlaymiz. “deshifrlash” bo’limiga kirish uchun ham sichqonchamiz chap tamonini ikki marta bosamiz yoki klaveturamizdan **Ctrl+D** tumasini bosamiz va quydagicha oyna hosil bo’ladi:



2.5-5-rasm.Deshifrlash bo’limini ochish oynasi.

Shundan keyin biz yuqoridagi kabi himoyalangan ma’lumotimizni ko’rsatamiz va uni tanlab **open** tugmasini bosamiz. Shunda bizga ma’lumot ochilganligi haqida xabar keladi:

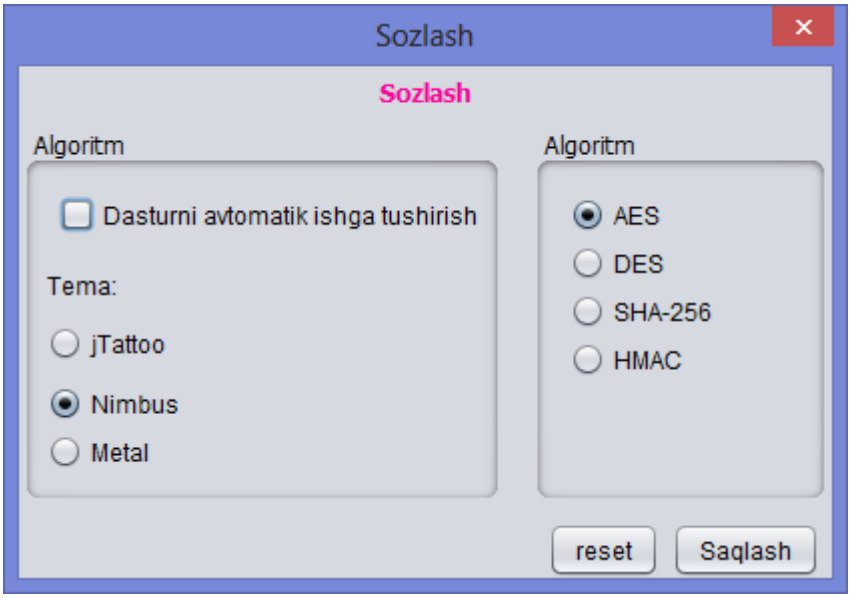


2.5-6-rasm.Ma’lumotni himoyasi ochilgani haqida xabar beruvchi oyna.

Ok tugmasini bosamiz va ma’lumotimiz asl holiga qaytadi.

Endi “sozlash” bo’limiga o’tamiz. Bu bo’lim asosiy bo’lim hisoblanadi ya’ni biz ma’lumotimizni qaysi algoritmda himoyalshimiz va boshqa jarayonlar amalga oshiriladi.

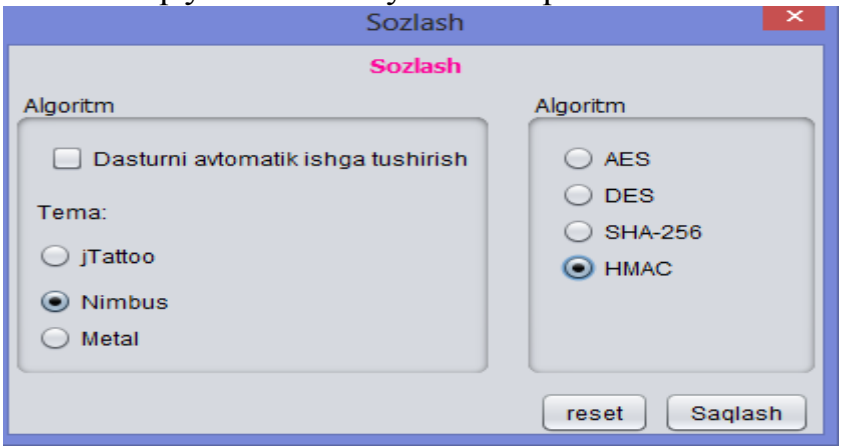
“sozlash”ni ochish uchun ham sichqonchamiz chap tamoni ikki marta bosiladi yoki klaveturamizdan **Ctrl+S** tugmasi bosiladi va quydagicha oyna hosil bo’ladi:



2.5-7-rasm. Sozlash bo’limi oynasi.

Biz ko’rib turgan oynamizning o’ng tamonida shifrlash algoritmlarining turlari berilgan. Shulardan birini tanlab ma’lumotimizni himoyalaymiz. Hozir dasturimiz AES algoritimida shifrlaydi.

Bundan tashqari DES, SHA-256 va HMAC algoritmlaridan ham foydalanamiz. Bu algoritmlardan qaysi biridan foydalanmoqchi bo’lsak ular ustiga sichqonchamizni bir



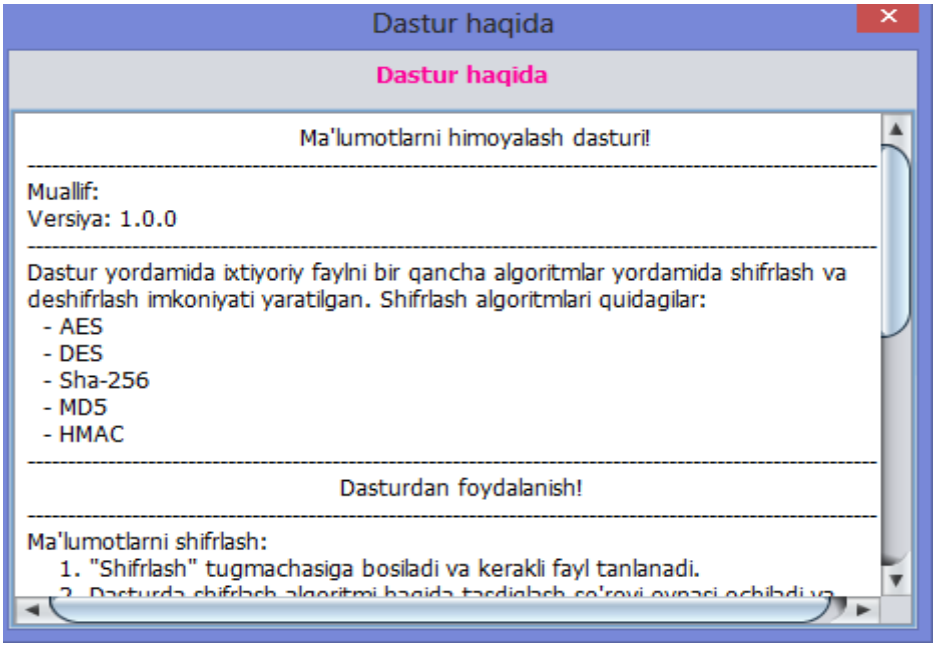
marta bosib tanlaymiz va **saqlash** ga bosamiz. Masalan

HMAC ni tanlab ko’ramiz:

2.5-8-rasm. Sozlash bo’limi oynasi.

So’ngi bo’limimiz bu “dastur haqida” gi bo’lim hisoblanada. Buda bizga dasturimiz haqida ma’lumotlar keltirilib o’tiladi.

Bu bo’limga kirish uchun ham avvalgilar kabi jarayon olib boramiz ya’ni sichqonchamizni dastur ustiga olib borib ikki marta bosamiz yoki klaveturamizdan **Ctrl+I** bosamiz va bizga quydagicha oyna hosil bo’ladi:



2.5-9-rasm. Dastur haqida bo’limi oynasi.

va bu bo’limning ichida quydagicha izohlar keltirilgan:

Ma'lumotlarni himoyalash dasturi!

Muallif:

Versiya: 1.0.0

Dastur yordamida ixtiyoriy faylni bir qancha algoritmlar yordamida shifrlash va deshifrlash imkoniyati yaratilgan. Shifrlash algoritmlari quyidagilar:

- AES
- DES
- Sha-256
- MD5
- HMAC

Dasturdan foydalanish!

Ma'lumotlarni shifrlash:

1. "Shifrlash" tugmachasiga bosiladi va kerakli fayl tanlanadi.
2. Dasturda shifrlash algoritmi haqida tasdiqlash so'rovi oynasi ochiladi va bundan "Yes" tugmasi tanlanadi.
3. Natijada ko'rsatilgan fayl joylashgan katalogda enc_<fayl_nomi>.<kengayma> shifrlangan fayli hosil bo'ladi.

Ma'lumotlarni deshifrlash:

1. "Deshifrlash" tugmachasi bosiladi va shifrlangan fayl tanlanadi.
2. Agar amallar muvaffaqqiyatli bajarilsa, shifrlangan fayl joylashgan katalogda dec_<fayl_nomi>.<kengayma> deshifrlangan fayli hosil bo'ladi.

Dasturni sozlash:

1. "Sozlash" tugmasi tanlanadi.
2. Kerakli algoritm tanlanadi va saqlash tugmasi bosiladi.

Tezkor tugmachalar:

* ctrl+e -> shifrlash
* ctrl+d -> deshifrlash
* ctrl+s -> sozlash
* ctrl+i -> dastur haqida

FOYDALANILGAN ADABIYOTLAR

1. I.Karimov O'zbekiston XXI - asr bo'sag’asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqiyot kafolatlari. Toshkent. 1997 y.
2. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Триумф-2002.
3. Майкл Ховард, Девид Лебланк. Защищенный код. Москва 2004.
4. Д. Скляров. Искусство, защиты и взлома информации. Санкт-Петербург. БХВ-Петербург. 2004.
5. Роберт Чёрчхаус. Коды и шифры. Москва 2006.
6. В. В. Ященко. Введения в криптография. Москва 2006.

7. Ж. Брассар. Современная криптология. Москва 2006.

8. В. Громов, Г.А. Васильев Энциклопедия компютерной безопасносты. Москва 2007.

9. Баричев С., Гончаров В.В., Серов Р.Е. Основы современной криптологии. Москва. Горячая линия. Телетом 2001 г/

Ю.Ганиев С.К., Каримов М.М. Х,исоблаш тизимлари ва тармокдарида информация химояси: Олий укув юрт. талаб. учун укув кулланма. - Тошкент давлат техника университети, 2003. 77б.

11. Шеннон К. Работы по теории информации и кибернетики / Пер. с англ. - М.: Иностранная литература, 1963. - 829с.

12. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.-М.: Гелиус АРВ, 2001.- 480 с.

13. Кан Д. Взломщики кодов. -М.: Издательство ”Центрполиграф“, 2000. - 473 с.

14. Завгородний В.И. Комплексная защита информации в компютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

15. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.

16. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.

17. Коблиц Н. Курс теории чисел в криптографии. - М., Научное издательство ТВП, 2001й.

18. Масленников А. Практическая криптография BHV - СПб 2003й.

19. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.

20. A. Ismoilov, Q. Usmonov. Hayot faoliyati xavfsizligi. O'quv qo'llanma. Samarqand - 2010

21.O.Qudratov, T. G’aniev. Hayotiy faoliyat xavfsizligi. Toshkent, 2004 y.

22. X.Rahimova va boshqalar. Mehnatni muhofaza qilish. Toshkent, 2004 y.

23. M.A.Qudratov va boshqalar. Hayotiy faoliyat xavfsizligi (ma’ruza kursi).

Toshkent, 2005y.

24. ftp: //ftp. kiae. su/msdos/crypto/pgp
25. http://drago.centerline.com:8080/franl/pgp/...
26. Yahoo - Computers, Security-and-Encryption
27. http://gov.uz