

VISUAL C++ MUHITIDA AXBOROTNI VIJINER USULIDA SHIFRLOVCHI VA DESHIFRLOVCHI DASTUR TUZISH

Shodimurodov Ulug'bek Akmalovich, Jo'rayev Asom Qo'yiliboy o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Nurafshon filiali, talaba

Annotasiya: Ushbu maqolada visual C++ muhitida axborotni vijiner usulida shriftlovchi va deshriftlovchi dastur tuzish haqida so'z boradi. Bizning oldimizda algoritmlarni EHM tushunadigan tilda yozish masalasi turadi, buning uchun maxsus algoritmik tillar mavjud.

Kalit so'zlar: EHM, PASKAL, programmalash, algoritmik,

EHM paydo bo'lganidan beri juda ko'plab algoritmik tillar yaratilgan. Ularni shartli ravishda uch tipga ajratish mumkin:

- Quyi darajadagi programmalash tillari (mashina tillari)

O'rta darajadagi programmalash tillari - Yuqori bosqichli programmalash tillari

Quyi darajadagi programmalash tillarida buyruqlar va amallar ma'lum kodlar (raqamlar) bilan ifodalangan bo'lib, ular EHM qurilmalari adreslari bilan bevosita ishlashga mo'ljallangan va mashina tili deb ham yuritiladi. O'rta darajadagi programmalash tillarida amallar va buyruqlarni (komandalar)ni ifodalash uchun odam tushinishi uchun qulay bo'lgan har xil qisqartma so'zlardan foydalaniladi. Bunda ham programma tuzuvchi EHM qurilmalari adreslari bilan ishlashi lozim. Bu qisqartmalar-mnemokodlar deyiladi, bu turdagi programmalash tillari assemblerlar deb ataladi.

Yuqori darajadagi programmalash tillarida ko'rsatmalar inson tiliga yaqin bo'lgan so'zlar va birikmalardan iborat bo'lib, programma tuzish uchun juda qulay va biror maxsus amallardan tashqari hollarda adreslar va qurilmalar bilan bevosita bog'liq ko'rsatmalarni bilish zarur emas. Yuqori bosqich programmalash tillariga misol sifatida FORTRAN, Algol, RL-1. BASIC, PASCAL, C, C++ tillarini keltirish mumkin

Informatsion texnologiyalarining jadal suratlar bilan rivojlanishi,

Internetning paydo bo'lishi, yangidan yangi va ma'lum maqsadlarga mo'ljallangan programmalash tillari va muhitlari yaratildi va yaratilmoqda.

Ulargamisol sifatida dBase, KARAT, LISP, FoxPro, Simula, Delphi, Visual Basic, Visual C++, HTML, Java, Java Script kabi tillar va programmalash muhitlarini keltirish mumkin. Hozirgi kunga kelib ob'ektga yo'naltirilgan va vizual programmalash texnologiyalari keng tarqalmoqda.

Himoyalangan axborotlarni ochishda deshifrlash jarayoni bo'lib bu maxfiylashgan axborotni ochishib o'qishda qo'l keladi Buning uchun bizga asosan kalit kerak bo'ladi. Kalit asosan "so'z" ya'ni harflardan iborat ko'rinishida bo'lib bu axborotni himoyalashda va uni ochishda kerak bo'ladi. Agar kalitni bilmagan odam bu axborotni qo'lga tushsa bu so'zning nima haqda ekanligini bilaolmaydi.

Bu mavzuning asosiy vazifasi ham anashunda hisoblanadi. Axborot faqat kelishilgan tomonlar tarafidan o'qiy olish mumkin.

Qadimgi urush davrlarda ham axborotlar dushman qo'lga tushib qolishi mumkinligini hisobga olib axborotlarni himoyalangan holda aloqa qilishgan. Kalit faqat axborotni qabul qilishi kerak bo'lgan tomon va axborotni yuborgan tomon tarafi biladi. Shuning uchun ham bu hatni kelishilgan tomonlar o'qiy oladi. Bu mavzuning afzalligi shundaki Vijnier usuli shifrlash usullari ichida eng himoyalangan usul hisoblanadi, bu shift kaliti "kalit so'z" ko'rinishida bo'ladi. Shifrlashni amalga oshirishda ochiq tekst va ochiq kalit kerak bo'ladi.

Bizga Mat berilgan bo'lsin bu matnni shifrlash uchun avvalo kalit so'z kerak. Bu kalit so'z yordamida berilgan matnni shifrlaymiz Vijnier shifrini ishlash prinsiping asosini misol yordamida ko'radigan bo'lsak "ABCDEF" so'zini kalit so'z deb qaraydigan bo'lsak, berilgan "TATU URGANCH FILIALI" so'zini shifrlash uchun kalit so'zdagi harflar bilan ishlaydi va quyidagicha shifrlaydi "TBVX YWGBEK JNLJCOM". Endi biz yashirilgan ya'ni shifrlangan axborotni ochishimiz uchun berilgan matnni teskari tartibda shu kalit so'z yordamida deshifrlaymiz.

Endi menga berilgan bu Vijnier usulida shifrlash va deshifrlash jarayonini dasturini tuzish vazifasi yuklatilgan bo'lib, men bu dasturni Visual C++ 2010 Windows Form da dasturini yaratdim.

Visual C++ 2010 dasturida bunday dasturlarni yaratish juda oson hisoblanadi negaki bu dasturda tayyor komponentalar mavjud bo'lib biz bundan to'g'ri foydalana bilsak eng yaxshi dasturni yarata olishimiz mumkin. Endi men bu dasturni yaratishimda kerak bo'ladigan komponentalar bilan tanishtirib chiqaman.

1. Form oynasi komponentalarni joylashtirish uchun oyna.

2. Button komponentasi bu komponentaning asosiy vazifasi shundan iboratki u orqali men shifrlash, deshifrlash, oynalami tozalash kalit so'z va matnlarni kiritishda kerak boladi.

3. Textbox komponentasi bu asosan text kiritishimizda va text xosil qilishimizda kerak bo'ladi.

4. Label komponentasi bu komponenta menga Form komponentalar- oynada nomini ko'rsatib berish uchun kerak yani nishon hisoblanadi.

5. Menu Strip bu komponenta menga fayl va yordam degan bo'limlarni qo'shishimda kerak bo'ldi.

6. Open file Dialog komponentasi bu komponenta menga txt faylni ochib berish va txt faylni saqlash uchun kerak bo'ldi.

Shular orqali bizning Vijiner shifrovchi va deshifrovchi dasturimiz yaratildi. Vijiner shifrlash usuli orqali biz muxim xabarlarini kalit so'z yordamida shifrlash va deshifrlash mumkin.

Internet texnologiyalarining yaratilish turli manbalardan tez va oson yo'l bilan axborot olish imkoniyatlarini hamma uchun oddiy fuqarodan tortib yirik tashkilotlarga misli ko'rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta'lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib, saqlay boshladilar.

Bu muhit avvalgi fizikaviy saqlashga nisbatan katta qulayliklar tug'diradi: saqlash juda ixcham, uzatish esa bir onda yuz beradi va tarmoq orqali boy ma'lumotlar bazalariga murojaat qilish imkoniyatlari juda keng. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko'payishiga olib keldi. Biznes qator tijorat soxalarida bugun axborotni o'zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo'lgan axborot haqida gap borganda o'ta ijobiy hodisa. Lekin pinhona (konfidensial) va maxfiy axborot oqimlari uchun Internet qulayliklari bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi.

Yuqorida yaratilgan Shifrlash- deshifrlash dasturi axborotni uzatish va qabul qilish ishlarida himoyalash maqsadida ishlatiladi. Ma'lumki hozirgi kunda ko'pgina sohalarda axborot eng qimmatli mulk hisoblanadi. Yaratilgan dastur bir oz bo'lsada yuborilayotgan matnli axborotni himoyalashga xizmat qiladi. Yuborilayotgan matnda albatta kalit ham joylashgan, lekin shifrlangan. matnni faqat shifrlash usulini va kalitni bilganlargina ochish imkoniyatiga ega bo'ladi. Vijiner shifrlash usulining qulayligi bu bizga yuborilayotgan ma'lumotni o'rta holatdagi ishonchlik bilan shifrlash mumkin. Ma'lumotlar bazasi, electron xujjatlar va boshqa maxfiy ma'lumotlarni shifrlash shifrovchi va deshifrovchi o'rtasida ma'lumotlarni ishonchli yo'l orqali yetkazish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Гради Буч. Объектно-ориентированный анализ и проектирование с примерами приложений на C++. Невский диалект, 560 стр. 2001 г.

2. Грехем И. Объектно ориентированные методы. Принципы практика. Вильямс. 879 стр, 2004 г.и



3. Иванова Г.С. Объектно ориентированное программирование Учебник. МГТУ им Баумана. 320 стр. 2003 г.
4. Фаулер М., Скотт К. UML в кратком изложении. Применение стандартного языка объектного моделирования. М., Мир, 1999.
5. Буч Г., Рамбо Д.,пользователя. М., ДМК, 2000. А. Язык UML: руководство Джекобсон
6. Пол Айра. Объектно-ориентированное программирование на C++. Второе издание. М.: Бином, 1999.