

«AMALIY MATEMATIKA VA AXBOROT TEXNOLOGIYALARINING ZAMONAVIY MUAMMOLARI»
XALQARO ILMIY-AMALIY ANJUMAN



TOSHKENT DAVLAT
TRANSPORT UNIVERSITETI
Tashkent state
transport university



BUXORO
DAVLAT
UNIVERSITETI



«AMALIY MATEMATIKA VA AXBOROT TEXNOLOGIYALARINING
ZAMONAVIY MUAMMOLARI»
XALQARO ILMIY-AMALIY ANJUMAN
MATERIALLARI

ABSTRACTS
INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE
«MODERN PROBLEMS OF APPLIED MATHEMATICS AND
INFORMATION TECHNOLOGIES»

МАТЕРИАЛЫ
МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
«СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРИКЛАДНОЙ МАТЕМАТИКИ И
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

2022-yil, 11-12 may



BUXORO – 2022



Buxoro davlat universiteti
BUXORO, 200117, M.IQBOL ko'chasi, 11-uy, 2022



@buxdu_uz



@buxdu1



@buxdu1



www.buxdu.uz

**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ
ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ФАНЛАР АКАДЕМИЯСИ
В.И. РОМАНОВСКИЙ НОМИДАГИ МАТЕМАТИКА ИНСТИТУТИ
ЎЗБЕКИСТОН МИЛЛИЙ УНИВЕРСИТЕТИ
ТОШКЕНТ ДАВЛАТ ТРАНСПОРТ УНИВЕРСИТЕТИ
БУХОРО ДАВЛАТ УНИВЕРСИТЕТИ**

Бухоро фарзанди, Беруний номидаги Давлат мукофоти лауреати, кўплаб ёш изланувчиларнинг ўз йўлини топиб олишида раҳнамолик қилган етук олим, физика-математика фанлари доктори Файбулла Назруллаевич Салиховнинг 90 йиллик юбилейларига бағишланади

**АМАЛИЙ МАТЕМАТИКА ВА
АХБОРОТ ТЕХНОЛОГИЯЛАРИНИНГ
ЗАМОНАВИЙ МУАММОЛАРИ**

**ХАЛҚАРО ИЛМИЙ-АМАЛИЙ АНЖУМАН
МАТЕРИАЛЛАРИ**

2022 йил, 11-12 май

БУХОРО – 2022

2. Zhang, X., Qi, L., Tang, Z., & Zhang, Y. (2014). Portable true random number generator for personal encryption application based on smartphone camera. *Electronics Letters*, 50(24), 1841–1843. <https://doi.org/10.1049/el.2014.2870>

AXBOROT TIZIMLARI FOYDALANUVCHILARINI FINGERPRINT YORDAMIDA BIOMETRIK AVTORIZATSIYADAN O‘TKAZISH

Salimov R.N.

*Buxoro davlat universiteti, Buxoro, O‘zbekiston
salimovruzibek283@gmail.com*

Foydalanuvchining shaxsini tasdiqlash uchun biometrik xavfsizlik tizimlari tabiatan insonga tegishli bo‘lgan tana a‘zolari – retinal tomirlar, barmoq izlari, kaft, qo‘l yozuvi, ovoz va boshqalardan foydalanadi. Ushbu ma‘lumotlarni kiritish odatiy parol o‘rnini bosadi. Kompyuter texnologiyalari sohasida sizning barmoq izingiz barcha turdagi sizga tegishli raqamli ma‘lumotlar bilan birlashtirish uchun unikal identifikatorlarni yaratish jarayonini anglatadi. Ammo individual foydalanuvchilarni yoki hisoblash qurilmalarini aniqlashning muayyan usullari haqida gap ketganda, biz raqamli barmoq izingiz bilan brauzer yoki qurilmaga murojaat qilamiz. Biometrik avtorizatsiyaning FingerPrint usulida barmoq izi shaxsiy kompyuterda tegishli shaxsning avval olingan barmoq izlari bilan solishtirish orqali aniqlanuvchi jarayon hisoblanib, shu jarayon natijasi ha (true) yoki yo‘q (false) javob sifatida qaytariladi.

So‘nggi paytlarda bunday barmoq izlari shaxsni aniqlash va kredit kartalaridagi firibgarlikni oldini olishda keng foydalanib kelinmoqda. 2017 yil boshiga kelib, barmoq izi foydalanilgan brauzer bilan cheklangan edi, shuning uchun brauzerni o‘zgartirish orqali barmoq izini o‘zgartirish oson edi. 2017-yilda bir xil qurilmada foydalanuvchini turli brauzerlardan kuzatish imkonini beruvchi kross-brauzer barmoq izi usuli chop etildi.

Qurilmaning barmoq izi tushunchasi inson barmoq izlarining amaliy ahamiyati bilan bog‘liq. Ideal holda, barcha mashinalar boshqa barmoq izi qiymatiga ega va bu qiymat hech qachon o‘zgarmaydi. Bunday holda, foydalanuvchining roziligisiz tarmoqdagi har bir mashinani unikal tarzda aniqlash mumkin bo‘ladi.

Barmoq izi tekshiriluv jarayoni faol va nafaol usulda amalga oshiriladi. Faol usulda barmoq izi mijoz so‘rovlarni amalga oshirishga ruxsat berishga asoslanadi. Ushbu usul eng keng tarqalgan usul bo‘lib, jarayon natijasi true qiymat qaytarsa mijoz mashinasiga faoliyat yuritishga ruxsat beriladi. Bunday ma‘lumotlar mualliflik huquqini himoya qilishning texnik vositalari sohasidagi dasturlar uchun foydalidir.

Shuningdek, ikki faktorli autentifikatsiya turi mavjud bo‘lib, unda ko‘pchilik o‘z qurilmalarini kirishdan himoya qilish uchun parollardan foydalanadi. Masalan turli gadgetlarda Touch ID yoki Face ID bo‘lmasa, bu xavfsizlik tizimi foydalauvchiga qurilmada ishlash ruxsatini bermaydi[2].

Ikki faktorli autentifikatsiya foydalanuvchini o‘z shaxsini ikki xil usulda tekshirishga majbur qiladi va bu qurilmani buzishni deyarli imkonsiz qiladi. Misol uchun, agar smartfon o‘g‘irlangan bo‘lsa va o‘g‘ri undan parol olishga muvaffaq bo‘lsa, uni qulf(blok)dan chiqarish uchun egasining barmoq izi ham kerak bo‘ladi. Birovning barmog‘ini sezilmas tarzda skanerlash va uning teriga yaqin materialdan o‘ta aniq 3D modelini yaratish kundalik darajada real bo‘lmagan jarayondir.

Bu kungi kunda biometrik xavfsizlikni tizimlarini chetlab o‘tish qiyin. Gap shundaki, yuqorida aytib o‘tilgan xususiyatlar har bir kishi uchun o‘ziga xosdir. Hatto yaqin qarindoshlar orasida ham barmoq izlari boshqacha bo‘ladi. Albatta, skaner ba‘zi xatolarga yo‘l qo‘yadi, lekin o‘g‘irlangan qurilmaning biometrik ma‘lumotlari egasining ma‘lumotlari bilan 99,99% bir xil bo‘lgan shaxsga yetib borishi ehtimoli deyarli nolga teng.

Foydalanilgan adabiyotlar

1. Саломатин А. А., Исхаков А.Ю. Применение интегрированного показателя отпечатков браузера в задаче адаптивной аутентификации субъектов доступа // Информационные и математические технологии в науке и управлении. 2020. №4 (20).
2. Шафиев Т. Р. [и др.]. Проектирование национальной системы управления персональной библиографической информацией // Проблемы вычислительной и прикладной математики. 2021. (5(35)). С. 44–51.

AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH MAVZUSI AMALIY MASHG‘ULOTNI TASHKIL QILISH KEYS-STADI METODIDAN FOYDALANISH.

Tahirov B.N.

Buxoro davlat universiteti, Buxoro, O‘zbekiston

Keys-stadi metodidan foydalanib amaliy mashg‘ulotlarni tashkil qilish.

Keys-stadi metodi

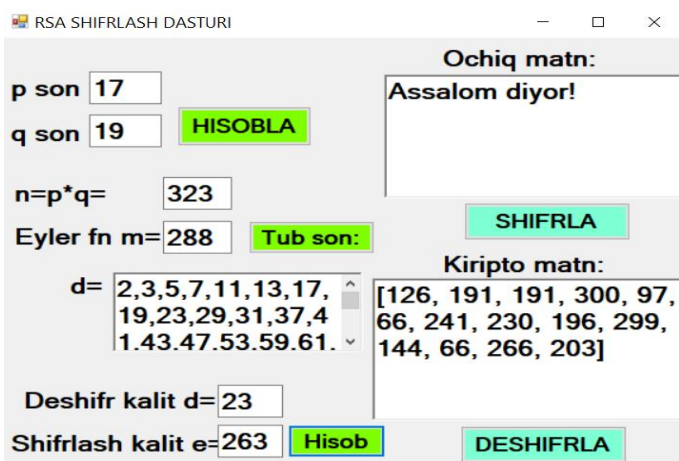
Bu metodning nomi inglizcha “**case-study**” soʻzlaridan olingan. Bunda “**case**” – yashik, quti, “**study**” – oʻrganish, tadqiq qilish, ilm bilan shugʻullanish, oʻquv fani, saboq olish, oʻqish maʼnolarini bildiradi. Bu metodni “**Amaliy holatlarni oʻqitish metodi**” deb ham ataladi.

“**Kriptografiya**” atamasi yunon tilidan olingan boʻlib, “yashirish, yozuvni berkitib qoʻymoq, sirli yozuv” maʼnosini anglatadi.

1-Keys topshiriq: Microsoft Visual Studio muhitining WindowsFormsApplication C# dasturlash tilida RSA algoritmi loyihasini bajarish tartibi.

Microsoft Visual Studio muhitida loyiha yaratish uchun:

1. Microsoft Visual Studio ilovasini <https://visualstudio.microsoft.com> rasmiy saytida yuklaymiz va komputerrimizga oʻrnatamiz.
2. Microsoft Visual Studio ilovasini ishga tushiramiz.
3. Unda New Project->Visual C#-> WindowsFormsApplication ni tanlaymiz.
4. WindowsFormsApplicationning oynasi obyektlar joylashtiramiz
5. Dastur yozamiz.



1-rasm. RSA algoritmi dastur narijasi koʻrinish.

2-Keys topshiq: Guruh talabalari uchun individual keys topshirigʻi asosida bilimni tekshirish.

Amaliy ishni bajarishdan maqsad: Talalar axborotlarning kompyuter xotirasida qanday koʻrinishda kodlanishni oʻrganish.

Ishni bajarish uchun dastur namunasi:

```
s=input() # "Axborotni kiritish qabul qilish jarayoni"
n=int(len(s))
ss=""
for i in range (n):
    b=bin(ord(s[i]))
    b=b[2:]
    l=len(b)
    while (l!=8):
        b='0'+b
        l=l+1
    ss+=b
print(ss)
```

№	Axborot	ASCII oʻnlikdagi kodi	ASCII ikkilikdagi kodi
Misol uchun	Assalom	[65, 115, 115, 97, 108, 111, 109]	[01000001011100110111001 01100001 01101100 01101111 01101101]
1.	Axborot		
2.	Olam		
3.	Dunyo		
4.	Texnologiyar		

3 - Keys topshiq: Guruh talabalari uchun individual keys topshirigʻi asosida bilimni tekshirish.

Amaliy ishni bajarishdan maqsad: Talalar axborotlarni RSA algoritimida deshifrlashni o'rganish.

№	Shifrlangan xabar	Deshifrlash kaliti (d ; n)	
Misol	[65, 115, 115, 97, 108, 111, 109]	203 ; 323	
1.	[68, 111, 351, 115, 116, 108, 97, 114]	293 ; 437	
2.	[79, 108, 97, 109]	137 ; 299	
3.	[68, 117, 110, 121, 111]	31 ; 253	
4.	[103, 9, 420, 36, 171, 36, 261]	157 ; 551	

Xulosa qilib, axborot xavfsizligini ta'minlash usullarini 4 ta asosiy sinfga ya'ni tashkiliy usul, huquqiy usul, apparat-dasturiy usul, kriptografik usulga bo'linadi. Axborot xavfsizligini ta'minlashning eng arzon va samarali usuli bo'lib aynan kriptografik usul hisoblanadi. Shu sababli bu usul amaliyotda, elektron raqamli imzoda va dunyo miqiyosida keng qo'llanilib kelinmoqda. Talabalarga bu kriptografik shifrlash algoritmlarining nazariy va amali jihat keys topshiriqlar bilan o'rgatish, bo'lajak axborot texnologiyalari mutaxasislari uchun juda muhim hisoblanadi.

FOYDALANILGAN ADABIYOTLAR.

- Behzod Takhirov, Алгоритмы шифрования и их свойства// Universum: технические науки № 11 (92), ноябрь, 2021 г. С.66-68.
- Хаятов Х.У., Тахиров Б.Н. Постановка обратной задачи для уравнений математической физики// Academy. № 10 (61), 2020. С.32-35.
- Тахиров Б.Н, Понятие виртуальной реальности // Наука, образование и культура. № 8 (52), 2020. С.12-15.

СТАНДАРТЛАРИДАГИ АЛГОРИТМЛАРИНИ ҚЎЛЛАБ-ҚУВВАТЛАЙДИГАН КРИПТОПРОВАЙДЕРНИНГ ИМКОНИАТЛАРИ

Алаев Р.Х.

Ўзбекистон Миллий университети, Тошкент, Ўзбекистон

Жаҳонда ахборот тизимлари ҳамда улардаги ахборотнинг хавфсизлигини таъминлаш усуллари, алгоритмлари ва тизимларини ишлаб чиқишга йўналтирилган илмий тадқиқотлар олиб борилмоқда. Хорижда Windows операцион тизими учун мўлжалланган дастурий воситаларда кriptografik амалларни бажаришда асосан криптопровайдерлардан фойдаланилади. Microsoft томонидан ишлаб чиқарилган барча дастурий воситаларда кriptografik амаллар криптопровайдерлар орқали амалга оширилади. Хорижий давлатларда ахборотнинг кriptografik муҳофазаси учун “Microsoft Primitive Provider”, “Microsoft Software Key Storage Provider”, “Microsoft SSL Protocol Provider”, “Microsoft Smart Card Key Storage Provider” номли CNG криптопровайдерлари (Microsoft, АКШ), “ViPNet CSP” (ИнфоТеКС, Россия), “КриптоПро CSP” (КриптоПро, Россия), “Signal-COM CSP” (Сигнал-КОМ, Россия), “Валидата CSP” (Валидата, Россия), “Лисси CSP” (ЛИССИ-Софт, Россия), “Tumar CSP” (Гамма Технологиялар, Қозоғистон), “AVEST CSP” (АВЕСТ, Белоруссия), “ИТ” (ИТ, Украина) криптопровайдерлари яратилган.

Мамлакатимизда қабул қилинган О‘зДСт 1106:2009, О‘зДСт 1105:2009 ва О‘зДСт 1092:2009 миллий стандартларидаги алгоритмларини қўллаб-қувватлайдиган «ARH Primitive Provider» Ва «ARH Key Storage Provider» номли криптопровайдерлар яратилди. Ушбу криптопровайдерлар ва уларнинг ёрдамчи модуллари қуйидаги имкониятларни тақдим этади:

- О‘зДСт 1092:2009 стандартидаги алгоритмларнинг жуфт калитларини яратиш, экспорт/импорт қилиш, қўллаш ва ўчириш.
- ПИН-код асосида аутентификациялаш.
- ПИН-кодсиз аутентификациялаш.
- Фойдаланувчининг кriptografik калитларини қўллаб-қувватлаш.
- О‘зДСт 1092:2009 стандартининг алгоритмлари билан имзони шакллантириш ва текшириш, О‘зДСт 1105:2009 ва ГОСТ 28147-89 стандартларининг алгоритмлари билан симметрик шифрлаш, О‘зДСт 1106:2009 стандартининг алгоритмлари билан маълумотларни хэшлаш.
- Операцион тизим сервис дастурлари учун кriptografik амалларни тақдим этиш.
- Операцион тизимнинг О‘зДСт 1106:2009 ва О‘зДСт 1092:2009 алгоритмлари асосида яратилган рақамли сертификатлар билан ишлашини таъминлаш.

Salimov R.N. AXBOROT TIZIMLARI FOYDALANUVCHILARINI FINGERPRINT YORDAMIDA BIOMETRIK AVTORIZATSIYADAN O‘TKAZISH	466
Tahirov B.N. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH MAVZUSI AMALIY MASHG‘ULOTNI TASHKIL QILISH KEYS-STADI METODIDAN FOYDALANISH.	466
Алаев Р.Х. СТАНДАРТЛАРИДАГИ АЛГОРИТМЛАРИНИ ҚЎЛЛАБ-ҚУВВАТЛАЙДИГАН КРИПТОПРОВАЙДЕРНИНГ ИМКОНИАТЛАРИ	468
Ёркулов Б.А. МЕТОДИКА ОЦЕНКИ ИМЕЮЩЕГОСЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ.....	469
Мнухин В. Б. МЕТОДЫ ЗАЩИТЫ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ КОНЕЧНЫХ ПОЛЕЙ ГАУССА И ЭЙЗЕНШТЕЙНА	470
Хазратов Ф.Х., Гадоева М.В. АЙРИМ НОСИММЕТРИК КРИПТОАЛГОРИТМЛАРНИ ТАКОМИЛЛАШТИРИШ	471

VIII ШЎҒБА. ТАЪЛИМДА РАҚАМЛИ ТЕХНОЛОГИЯЛАР. DIGITAL TECHNOLOGIES IN EDUCATION.....

Abdullayeva N.I. KOMPYUTER INJINIRINGI YO‘NALISHIDA “DISKRET TUZILMALAR” KURSINI O‘QITISHNING METODIK TA‘MINOTI SIFATIDA MOBIL ILOVA LOYIHASI	473
Abdullayeva Z.G`. TA‘LIM JARAYONIDA DROPBOX PLATFORMASIDAN FOYDALANISH	474
Abdullayeva Z.G`. FIZIKA FANINI O‘QITISHDA AXBOROT-KOMMUNIKATSION TEXNOLOGIYALARDAN FOYDALANISH.....	475
Abdurazakov A., Mirzamahmudova N., Mahmudova N. IQTISODIYOT YO‘NALISHIDAGI TALABALARNING MUTAXASSISLIK FAOLIYATIDA INFORMATSION TEXNOLOGIYADAN FOYDALANISH KOMPETENTLIGINI OSHIRISH	475
Abidov K.Z., Ismatova K.O. TRANSPORT MASALASINI KOMPYUTERLI MODELLASHTIRISHDA INTERFEYSNI TANLASH	477
Abidov K.Z., Shamsiyeva N.R. SIMPLEKS USULINI KOMPYUTERLI MODELLASHTIRISHDA RANGLASH EFFEKTLARIDAN FOYDALANISH.....	478
Alqarov I.SH., Ergashev E.K. TALABALARNI IJTIMOIIY FAOL SHAXS QILIB SHAKLLANTIRISH MODELII MAZMUNINI TALABALAR ONGIGA SINGDIRISHNING TIZIMII YONDASHUVI ..	479
Bahodirov M.D., Turdiyev A.P. WEB DASTURLASHDA — PHP.....	480
Bahromova M.M. BOLALARDA RAQAMLI TAFAKKURNI RIVOJLANTIRUVCHI VOSITALAR	481
Bahronova D.M. ILMIY JURNALLAR UCHUN OCHIQ JURNAL TIZIMLARI HAQIDA VA ULARNI JORIY ETISH ISTIQBOLLARI	482
Baxromova S.B. FOKS FUNKSIYASIGA OID	483
Bo`ronova G.Y., Qahhorova M.B. UMUMTA‘LIM MAKTABLARIDA ROBOTOTEXNIKANI FAN SIFATIDA O‘QITISHNING DOLZARBLIGI.	483
Daliyev Sh.K., Eshonqulov E.Sh., Soliyev S.O`. TA‘LIM YO‘NALISHLARI UCHUN TEXNOLOGIK XARITALARNI SHAKLLANTIRISHDAGI YONDASHUV	484
Daliyev Sh.K., Mustafojev E.M. BRAYL ALIFBOSINI TANIB OLI SHDAGI YONDASHUVLAR .	485
Elmurodov K.Q. MATEMATIKA FANINI O‘QITISHDA ZAMONAVIIY AXBOROT TEXNOLOGIYALAR O‘RNI	487
Fayziyeva D.H., Yahyayeva Sh.T. RAQAMLI TA‘LIMNI JALB QILISHNING TALABALAR MUVAFFAQIYATIGA TA‘SIRI.....	487
Ibroximov S.R. MOBIL TA‘LIMNING AFZALLIKLARI VA KAMCHILIKLARI	488
Imomova Sh.M., Qosimova Y.A. TA‘LIM TIZIMIDA GOOGLE BULUTLI XIZMATLARIDAN FOYDALANISH	489
Jo‘rakulov T.T. O‘QUV JARAYONINI MATEMATIK MODELII ASOSIDA HISOBLASH TAJRIBALARI	489
Jo‘rayeva N.O. MUSTAQIL TA‘LIMNI TASHKIL ETISH USULLARI	490
Karimov Q.M. MAPLE AMALIY DASTUR PAKETINING GRAFIK IMKONIYATIDAN TENGLAMALARNI YECHISHDA FOYDALANISH.....	491
Kęsik J., Szymczyk T., Montusiewicz J., Samarov Kh., Abdullayev U. DIGITAL DOCUMENTATION OF MONUMENTS – MODERN INFORMATION TECHNOLOGIES AND METHODOLOGIES.....	492
Kodirov Z.Z., Inamova G.A., O‘rmonov M.N. ARDUINO PLATFORMASINI TA‘LIMDAGI O‘RNI	493
Matyakubov A.S., Esonmurodov S.Q., Tadjiyev R.N. TALABALARNI ISHGA JOYLASHISHIGA KO‘MAKLASHISH DASTURIDA PROFESSOR-O‘QITUVCHILARNING O‘RNI.....	494