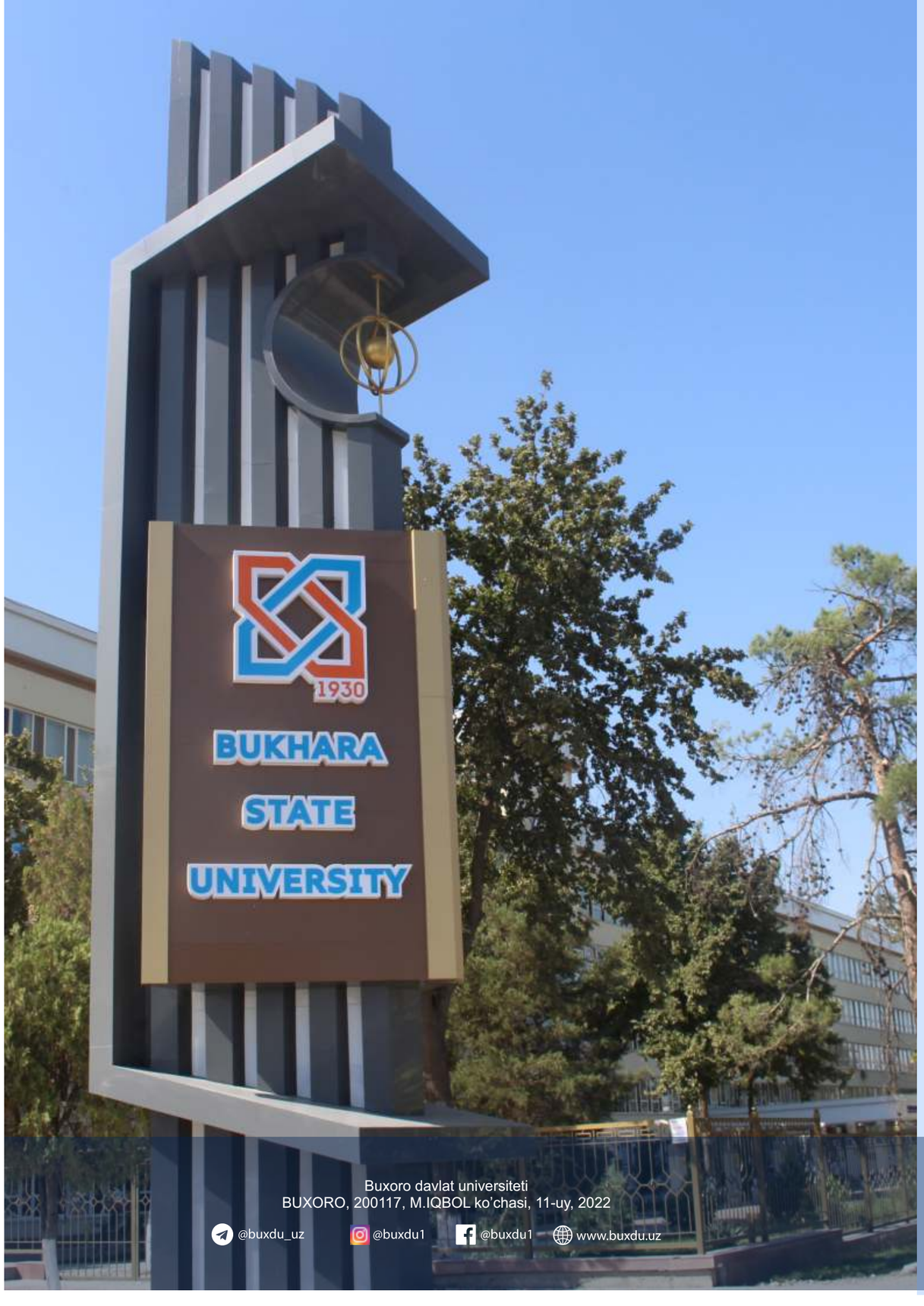


Buxoro davlat universiteti
BUXORO, 200117, M.IQBOL ko'chasi, 11-uy, 2022

@buxdu_uz @buxdu1 @buxdu1 www.buxdu.uz

«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

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 Ғайбулла 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 nofaol usulda amalga oshiriladi. Faol usulda barmoq izi mijoz so'rovlarni amalga oshirishga ruxsat berishiga asoslanadi. Ushbu usul eng keng tarqalgan usul bo’lib, jarayon natijasi true qimat 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

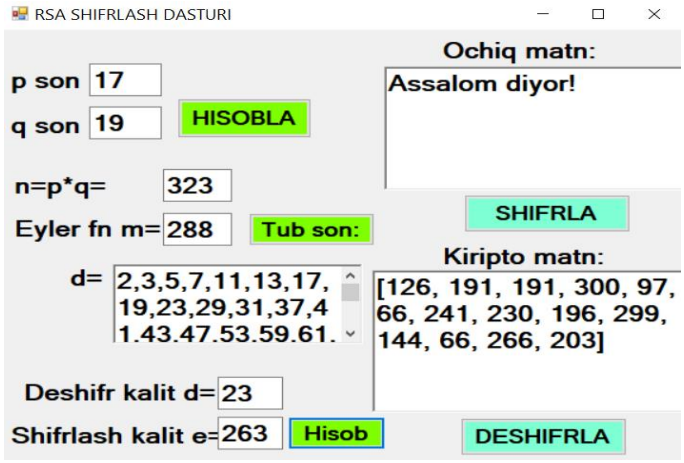
Bu metodning nomi inglizcha **“case-study”** so‘zlaridan olingan. Bunda **“case”** – yashik, quti, **“study”** – o‘rganish, tadqiq qilish, ilm bilan shug‘ullanish, o‘quv fani, saboq olish, o‘qish ma’nolarini bildiradi. Bu metodni **“Amaliy holatlarni o‘qitish metodi”** deb ham ataladi.

“Kriptografiya” atamasi yunon tilidan olingan bo’lib, “yashirish, yozuvni berkitib qo’ymoq, sirli yozuv” ma’nosini 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 o‘rnatamiz.
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 ko‘rinish.

2-Keys topshiq: Guruh talabalari uchun individual keys topshirig‘i asosida bilimini tekshirish.

Amaliy ishni bajarishdan maqsad: Talalar axborotlarning kompyuter xotirasida qanday ko‘rnishda kodlanishni o‘rganish.

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 o‘nlikdagi kodi	ASCII ikkilikdagi kodi
Misol uchun	Assalom	[65, 115, 115, 97, 108, 11 109]	[0100000101110011011100 1 01100001 01101100 01101111 01101101]
1.	Axborot		
2.	Olam		
3.	Dunyo		
4.	Texnologiyar		

3 - Keys topshiq: Guruh talabalari uchun individual keys topshirig‘i asosida bilimini 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 kiptografik usul hisoblanadi. Shu sababli bu usul amaliyotda, ellektron raqamli imzoda va dunyo miqiyosida keng qo‘llanilib kelinmoqda. Talabalarga bu kriptografik shifrlash algoritimlarining nazariy va amali jihat keys topshiriqlar bilan o‘rgatish, bo‘lajak axborot texnologiyalari mutaxasislari uchun juda muhim hisoblanadi.

FOYDALANILGAN ADABIYOTLAR.

1. Behzod Takhirov, Алгоритмы шифрования и их свойства// Universum: технические науки № 11 (92), ноябрь, 2021 г. С.66-68.

1. Хаятов Х.У., Тахиров Б.Н. Постановка обратной задачи для уравнений математической физики// Academy. № 10 (61), 2020. С.32-35.

2. Тахиров Б.Н, Понятие виртуальной реальности // Наука, образование и культура. № 8 (52), 2020. С.12-15.

СТАНДАРТЛАРИДАГИ АЛГОРИТМЛАРИНИ ҚЎЛЛАБ-ҚУВВАТЛАЙДИГАН КРИПТОПРОВАЙДЕРНИНГ ИМКОНИЯТЛАРИ

Алаев Р.Ҳ.

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 криптографик амалларни бажаришда асосан криптопровайдерлардан фойдаланилади. Microsoft томонидан ишлаб чиқарилган барча дастурий воситаларда криптографик амаллар криптопровайдерлар орқали амалга оширилади. Хорижий давлатларда ахборотнинг криптографик муҳофазаси учун “Microsoft Primitive Provider”, “Microsoft Software Key Storage Provider”, “Microsoft SSL Protocol Provider”, “Microsoft Smart Card Key Storage Provider” номли CNG криптопровайдерлари (Microsoft, АҚШ), “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), "IIT" (IIT, Украина) криптопровайдерлари яратилган.

Мамлакатимизда қабул қилинган O‘zDSt 1106:2009, O‘zDSt 1105:2009 ва O‘zDSt 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:

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