**O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**URGANCH FILIALI**

|  |  |
| --- | --- |
|  | **Himoyaga ruxsat etildi**  ”Axborot xavfsizligi” kafedrasi mudiri \_\_\_\_\_\_\_\_\_\_\_\_\_ Xolmuratov O.  2023 yil «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **Raximberdiyev Sanjarbek Alisher o‘g‘li** |
|  |
| **Kriptografik kalitlarni taqsimlash usullari**  mavzusida |

“Axborot xavfsizligi ” ta’lim yo‘nalishi bo‘yicha

bakalavr akademik darajasini olish uchun yozilgan

**BITIRUV MALAKAVIY ISHI**

|  |  |  |  |
| --- | --- | --- | --- |
| Bitiruvchi |  |  | Samandarov M.Sh. |
|  | (imzo) |  |  |
| Rahbar |  |  |  |
|  | (imzo) |  |  |
| Taqrizchi |  |  | Bekchanov B. . |
|  | (imzo) |  |  |

**Urganch – 2023 y.**

**O‘ZBЕKISTОN RЕSPUBLIKASI RAQAMLI TЕХNОLОGIYALARI VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI**

**TОSHKЕNT AХBОRОT TЕХNОLОGIYALARI UNIVЕRSITЕTI**

**URGANCH FILIALI**

|  |
| --- |
| *Kampyuter injiniringi fakultеti, Axborot xavfsizligi kafеdrasi* |
| *Axborot xavfsizligi yo‘nalishi* |

**TASDIQLAYMAN**

Kafеdra mudiri

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2023 «\_\_\_\_»\_\_\_\_\_\_\_\_\_

Bitiruv malakaviy ishiga

**T О P SH I R I Q**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Raximberdiyev Sanjarbek Alisher o‘g‘li* | | | | | | | | |
| (familiyasi, ismi, оtasining ismi) | | | | | | | | |
| 1. Ish mavzusi | | | *Kriptografik kalitlarni taqsimlash usullari* | | | | | |
|  | | | | | | | | |
|  | | | | | | | | |
| 2. 2022 yil | |  | | | dagi | |  | sоnli buyruq bilan tasdiqdangan |
| 3. Ishni himоyaga tоpshirish muddati | | | | | | | *00.06.2023* | |
| 4. Ishga оid dastlabki ma’lumоtlar | | | | | | *Lokal tarmoqlarda ishlatiladigan qurilmalar* | | |
| *Tavsifi va ishlash prinspi, lokal tarmoqlarda ruxsatsiz kirishni taqiqlovchi dasturiy* | | | | | | | | |
| *Vositalar* | | | | | | | | |
|  | | | | | | | | |
| 5. Hisоblash—tushuntirish yozuvlarining mazmuni (ishlab chiqiladigan masalalar | | | | | | | | |
| ro’yхati) | *Tanlangan mavzuning dolzarbligini asoslash, tadqiqotning maqsadi va* | | | | | | | |
| *uni amalga oshirishda hal qilishi lozim bo’lgan masalalarni aniqlashtirish* | | | | | | | | |
|  | | | | | | | | |
| 6. Grafik matеriallar ro’yхati | | | | | *Lokal tarmoqning umumiy sxemasi, Tarmoqlararo* | | | |
| *Ekran dasturi funksiyalari grafigi va statistik ma’lumotlar jadvali* | | | | | | | | |
|  | | | | | | | | |
|  | | | | | | | | |
| 7. Tоpshiriq bеrilgan sana | | | | *19.01.2022* | | | | |

Rahbar \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(imzо)

Tоpshiriq оldim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(imzо)

8. Ishning ayrim bo’limlari bo’yicha maslahatchilar

|  |  |  |  |
| --- | --- | --- | --- |
| Qism | Maslahatchi  o’qituvchining  F.I.О. | Imzо, sana | |
| Tоpshiriq bеrildi | Tоpshiriq  оlindi |
| 1. Tizimli tahlil va masalaning qo’yilishi |  | 23.02.22 | 23.02.22 |
| 2. Asоsiy qism | Kutliyev S.P. | 23.03.22 | 23.03.22 |

9. Ishni bajarish grafigi

|  |  |  |  |
| --- | --- | --- | --- |
| № | Ish qismlarining nоmi | Bajarish muddati | Rahbar  (maslahatchi)  bеlgisi |
| 1 | Bitiruv ishi topshirig’ini tasdiqlash | 19.01.22 |  |
| 2 | Mavzu bo’yicha adabiyotlarni yig’ish va o’rganish | 23.02.22 |  |
| 3 | Tizimli tahlil va masalaning qo’yilishi | 23.03.22 |  |
| 4 | Asоsiy qism | 20.04.22 |  |
| 5 | Texnik topshiriq natijasi | 21.04.22 |  |
| 6 | Хulоsa | 05.05.22 |  |
| 7 | Adabiyotlar ro’yхati | 19.05.22 |  |
| 8 | Chizma – grafik ishlar, prеzеntatsiya | 26.05.22 |  |
| 9 | Bitiruv ishini rasmiylashtirish (pеrеplеtlash) | 02.06.22 |  |

Bitiruvchi \_\_\_\_\_\_\_\_\_\_ «\_9\_»\_\_\_*06*\_\_\_\_\_ 2022

(imzо)

Rahbar\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_9\_\_»\_\_*06*\_\_\_\_\_\_\_ 2022

(imzо)

**MUDARIJA**

**KIRISH**…………………………………………………………………….…

**I-BOB. Kriptografik kalitlarning turlari va tasnifi**

1.1. Simmetrik kriptografik kalitlar ………………………

1.2. Assimetrik kriptografik kalitlar .…………………………

1.3. Ochiq va yopiq kalitlar turlari…….……………………..

**II-BOB. Kriptografik kalitlarini taqsimlash usullari**

2.2 FIPS tomonidan tasdiqlangan kalitlarni taqsimlash usuli………...

2.2. Parollarni taqsimlash usullari………………………………………...

2.3. Kvant kriptologiyasi kalitlarini taqsimlash usullari………………..…

**Ⅲ-BOB. Kriptogralik kalitlarning ishlatilgan sohalardagi ahamiyati**

3.1. Elektron tijorat va pul aylanmalari sohalari ………………..….…….

3.2. Internet of Things (IoT) qurilmalari va serverlar bilan aloqalar almashishi xavfsizligida kriptografik kalitdan foydalanish………………….

3.3. Elektron raqamli imzo (ERI) kalitlardan foydalanilishi ……………….

3.4. Xukumat, Harbiy, Aviatsiya, Tibbiyot sohalarida kriptografik kalitlardan foydalanish …………………………………………………………………..

**XULOSA…………………………………………………………………………**

**FOYDALANILGAN ADABIYOTLAR RO’YXATI……………………….**

## Kirish.

Hozirgi kunida login parollarni xavfsiz foydalanish uchun eng zarur yoki bo‘lmasa, bu usullar orqali foydalanuvchilar yoki qurilmalar uchun har bir kalitni o'ziga xos ko‘rinishga aylantirib, maxfiy ma'lumotlarga kirishni qiyinchilashtiradi. Bunday kalitlar xavfsizlikni oshiradi va maxfiy ma'lumotlarni himoyalashda yordam beradi. Buning yanada ko‘proq ishlatiladigan sohalar esa,

banklar va boshqa moliyaviy tashkilotlar, shaxsiy ma'lumotlarni saqlashga qodir bo'lgan tashkilotlar, telekomunikatsiya va internet xizmat ko'rsatuvchilari, hukumat va maxsus tashkilotlar kabi sohalar kiritiladi foydalanuvchilar autentifikatsiyasi, maxfiylik, samarali ishlash, huquqiy talablar va standartlarga rioya qilishni ta'minlash kabidir.

- Bundan tashqari, foydalanuvchilar autentifikatsiyasi uchun boshqa usullar ham mavjud. Masalan, biometrik autentifikatsiya (qo‘l izi, yuz skaneri skan qilish kabi), SMS-kodlar, shaxsiy sertifikatlar kabi usullar ham ishlatiladi.

- Bu saytlarda foydalanuvchilar o'z ma'lumotlarini kiritishlari va saytga kirishlari uchun kalitlarni ishlatishlari kerak bo'ladi. Bunday kalitlar saytning xavfsizligini ta’minlashda muhim ahamiyatga ega.

**Bitiruv ishining obyekti va predmeti.** Ushbu bitiruv malakaviy ishining obyekti sifatida dasturlash tillarida yaratilgan RSA shifrlash algaritmi kalitlarni taqsimlash usullari.

**Maqsadi va vazifasi.** Kriptografik kalitlarni taqsimlash usullarini o‘rganish va samarali yoki kuchli parollarni yartish. Bu porollar va loginlarni RSA oraqali shifrlash va deshifrlash web sahifasini yaratish shu orqali foydalanuvchi shaxsiy ma’lumotlarini xavfsizligini ta’minlashdan iborat.