AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

XÜSUSİ TƏYİNATLI ELEKTRON SƏNƏD DÖVRİYYƏSİ SİSTEMLƏRİNDƏ İNFORMASİYANIN KONFİDENSİALLIĞININ QORUNMASI ÜSULLARI (TİBB MÜƏSSİSƏLƏRİ NÜMUNƏSİNDƏ)

İxtisas: 3338.01 – Sistemli analiz, idarəetmə və informasiyanın işlənməsi

Elm sahəsi: Texnika elmləri

İddiaçı: **Nərgiz Firuz qızı Məmmədzadə**

Fəlsəfə doktoru elmi dərəcəsi
almaq üçün təqdim edilmiş dissertasiyanın

AVTOREFERATI

Bakı – 2026

Dissertasiya işi Azərbaycan Texniki Universitetinin “Mühəndis riyaziyyatı və süni intellekt” kafedrasında yerinə yetirilmişdir.

Elmi rəhbər: Texnika elmləri doktoru, professor
Vaqif Əlicavad oğlu Qasımov

Rəsmi opponentlər: Texnika elmləri doktoru, professor
Ələkbər Əli Ağa oğlu Əliyev

Texnika elmləri doktoru, professor
Baləmi Qasım oğlu İsmayılov

Texnika elmləri doktoru, professor
Cavanşir Firudin oğlu Məmmədov

Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının Azərbaycan Dövlət Neft və Sənaye Universitetinin nəzdində fəaliyyət göstərən FD 2.48 Dissertasiya Şurası.

Dissertasiya Şurasının sədri: AMEA-nın müxbir üzvü, texnika elmləri doktoru, professor
Rafiq Əziz oğlu Əliyev

Dissertasiya Şurasının elmi katibi: texnika elmləri doktoru, dosent
Akif Vəli oğlu Əlizadə

Elmi seminarın sədri: texnika elmləri doktoru, professor
Kəmalə Rafiq qızı Əliyeva

İMZANI TƏSDİQ EDİRƏM
ADNSU-nun Elmi katibi

İŞİN ÜMUMİ XARAKTERİSTİKASI

Mövzunun aktuallığı və işlənmə dərəcəsi. Müasir dövrdə rəqəmsal texnologiyaların geniş yayılması və dövlət, özəl və hərbi sahələrdə elektron sənəd dövriyyəsi sistemlərinin tətbiqi informasiya təhlükəsizliyi məsələlərini ön plana çıxarmışdır. Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində (XTESDS) informasiyanın məxfiliyi, bütövlüyü və əlçatanlığı kritik əhəmiyyət daşıyır. Bu sistemlərdə informasiya təhlükəsizliyinin təmin edilməsi üçün müxtəlif kriptoqrafik üsulların, təhlükəsizlik protokollarının və təşkilati tədbirlərin tətbiqi vacibdir. Bu sahələrdən biri də tibbi müəssisələrdə generasiya edilən sənədlər və onların təhlükəsiz saxlanması, emalı və ötürülməsi prosesi ilə bağlıdır. Hal-hazırda XTESDS-də elektron sənədlərin təhlükəsizliyi üçün tətbiq olunan bir çox metodlar və üsullar mövcuddur. Lakin mövcud texnologiyaların zəif tərəfləri, eləcə də yeni yaranan kibertəhdidlər informasiya təhlükəsizliyi sahəsində əlavə tədqiqatların aparılmasını, yeni kriptoqrafik metodların və alqoritmlərin, təhlükəsizlik modellərinin işlənməsini və tətbiqini zəruri edir. Məlumatların icazəsiz əldə olunması, dəyişdirilməsi və ya məhv edilməsi dövlət və özəl strukturlar üçün ciddi fəsadlar törədə bilər. Bundan əlavə, rəqəmsal imza, elektron sənədlərin autentifikasiyası və mənbəyin identifikasiyası kimi aspektlər də XTESDS-nin təhlükəsizliyində mühüm rol oynayır.

Xüsusilə, tibbi elektron sənədlərdə informasiya təhlükəsizliyi məsələləri xüsusi əhəmiyyət kəsb edir. Pasiyentlərin sağlamlıq məlumatları konfidensial xarakter daşıyır, onların icazəsiz əldə olunması etik və hüquqi problemlərə səbəb ola bilər. Tibbi sənədlərin konfidensiallığının pozulması pasiyentin şəxsi həyatına müdaxilə olmaqla yanaşı, səhiyyə müəssisələrinin etibarına da xələl gətirə bilər. Bundan əlavə, səhiyyə sahəsində elektron sənəd dövriyyəsi sistemlərində təhlükəsizliyin pozulması nəticəsində səhv diaqnozların qoyulması, müalicə prosesinə müdaxilə və saxta reseptlərin yazılması kimi ciddi problemlər ortaya çıxa bilər. Bu sahədə beynəlxalq standartlar və normativ tələblər mövcuddur (ISO/IEC 27001, NIST 800-53, HIPAA və s.), lakin aparılmış

tədqiqatlar göstərir ki, bu standartların tam şəkildə yerinə yetirilməsi, onların tələblərinə riayət olunması üçün əlavə tədbirlərin görülməsinə zərurət vardır. Eyni zamanda, inkişaf etməkdə olan texnologiyalar, hesablama gucu, və mövcud metodların zamanla zəifliklərinin askarlanması yeni yanaşmaların işlənib hazırlanmasını tələb edir. Bu baxımdan, XTESDS-də, o cümlədən tibb müəssisələrində sənəd dövriyyəsi sistemlərində informasiya təhlükəsizliyinin təmin edilməsi üzrə effektiv həllərin işlənməsi və tətbiqi aktual elmi və praktiki problemlərdən biridir.

Dissertasiya işində tibb müəssisələri nümunəsində xüsusi təyinatlı elektron sənədlərin konfidensiallığının və təhlükəsizliyinin təmin edilməsi, tibbi sənədlərin saxlanılması, emalı və ötürülməsi üçün kriptoqrafik alqoritmlər, təhlükəsizlik model və arxitekturası, informasiyanın məxfiləşdirilməsi üsulları işlənmişdir.

Tədqiqatın obyekti tibb müəssisələrində elektron sənədlər nümunəsində xüsusi təyinatlı elektron sənəd dövriyyəsi sistemləridir.

Tədqiqatın predmeti tibbi sənədlərin konfidensiallığının və təhlükəsizliyinin təmin edilməsi üçün üsulların, alqoritmlərin, model və arxitekturaların yaradılmasından ibarətdir.

Tədqiqatın məqsədi və vəzifəsi: Tibb müəssisələrində elektron sənədlərin saxlanması, emalı və ötürülməsi proseslərində konfidensiallığı təmin etmək üçün kriptoqrafik alqoritmlərin, açar mübadiləsi protokollarının, paylanmış arxitekturlu məlumat bazaları üçün arxitektur modellərin, gizliliyi qorumaq üçün anonimləşdirmə alqoritmlərinin, sistemə və resurslara müraciət texnologiyalarının işlənməsindən ibarətdir.

Tədqiqat metodları: Təqdim olunan dissertasiya işində aparılan tədqiqatlarda xaotik nəzəriyyəsindən, təsadüfi ədədlər nəzəriyyəsindən, matrislər cəbrindən, statistik analiz üsullarından və eksperimental tədqiqatlardan istifadə edilmişdir.

Tədqiqatın nəzəri və praktiki əhəmiyyəti.

Tədqiqatın nəzəri və praktiki əhəmiyyəti irəli sürülən yanaşmaların həm fundamental, həm də tətbiqi xarakter daşıması ilə səciyyələnir. Belə ki, molekulların xaotik Broun hərəkəti və DFS alqoritmi vasitəsilə formalaşdırılmış qeyri-ənənəvi kriptoqrafik zəmin, həmçinin sinqulyar matrislərin dekompozisiyasına söykənən

alternativ açar mübadiləsi protokolu məlumatların şifrələnməsi və həssas tibbi məlumatların onların analizinə imkan vermə şərti ilə etibarlı anonimləşdirilməsi üçün yeni riyazi mühit yaratmaqla bərabər, onların real bazalarda qorunmasını və şəbəkələrdə təhlükəsiz ötürülməsini təmin edir. Eyni zamanda, lidersiz paylanmış sistemlərdə tranzaksiyaların sinxronizasiyası üçün təklif edilən yeni idarəetmə modelləri həm məlumat konfliktlərinin nəzəri həllini təkmilləşdirir, həm də tranzaksiyalar cədvəli əsaslı arxitektura vasitəsilə şəbəkə yükünü azaldaraq resursların praktiki optimallaşdırılmasını (replikasiyasını) və xətaya dözümlülüyü reallaşdırır.

Müdafiəyə çıxarılan əsas müddəalar:

- Mətn formatlı sənədlər üçün şifrləmə alqoritmi;
- Təsvir formatlı məlumatlar üçün kriptoqrafik şifrələmə alqoritmi;
- Şəbəkələrdə məlumat ötürülməsi zamanı kriptoqrafik açarların mübadiləsi protokolu;
- Verilənlərin analizi üçün konfidensial məlumatların anonimləşdirilməsi üsulu və alqoritmi;
- Paylanmış verilənlər bazaları üçün sinxronlaşdırma və replikasiya arxitekturası;
- Sənədlərin uzaq məsafəli bazalara ötürülməsi zamanı təhlükəsiz ötürülmə kanallarının yaradılması üsulu;
- Resurslara müraciət zamanı autentifikasiya və avtorizasiya modelləri.

Tədqiqatın elmi yeniliyi:

- Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemləri üçün paylanmış arxitekturlu model və paylanmış strukturlu xüsusi təyinatlı verilənlər bazaları arasında konfidensial informasiya mübadiləsinın konseptual prinsipləri təklif edilmişdir.
- Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində mətn tipli məlumatların (sənədlərin) konfidensiallığının təmin edilməsi üçün molekulların Broun xaotik hərəkəti modelinə əsaslanan təsadüfi ədədlərin generasiyası ilə yeni şifrələmə üsulu işlənmişdir.

- Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində təsvir (qrafik, şəkil) tipli məlumatların (sənədlərin) konfidensiallığının təmin edilməsi üçün DFS alqoritmi ilə generasiya edilən labirint əsaslı yeni şifrləmə alqoritmi işlənmişdir.
- Paylanmış strukturlu verilənlər bazası şəbəkəsində məlumatların ötürülməsi zamanı gizliliyin təmin edilməsi üçün matrislər cəbrinə əsaslanan xüsusi açar mübadiləsi protokolu işlənmişdir.
- Elektron sənəd dövriyyəsi sisteminin verilənlər bazalarında saxlanılan məlumatların istifadəsi zamanı anonimliyin təmin edilməsi üçün labirint generasiyasına əsaslanan xüsusi qarışdırma aloqritmi işlənmişdir.
- Paylanmış strukturlu verilənlər bazalarında sinxronlaşdırma və replikasiyanı təmin etmək üçün tranzaksiyalar cədvəlinin istifadəsi prinsipləri təklif edilmişdir.
- Verilənlər bazalarında saxlanılan məlumatlara girişin idarə edilməsi üçün dinamik rollar və icazələr yanaşması təklif edilmişdir.

Aprobasiyası və tətbiqi. Dissertasiya işinin əsas nəticələri aşağıdakı elmi-texniki konfrans və forumlarda müzakirə edilmişdir:

- Gasimov A. Vagif, Mammadov I. Jabir, Mammadzada F. Nargiz , Stream Encryptıon Method Based On The Chaotıc Brownıan Motıon Model of Molecules / Procedia Computer Science, vol. 215, 2022, p.p. 577-588. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.060. (https://www.sciencedirect.com/science/article/pii/S1877050922021317);

- Gasimov, Vagif & Mammadzada, Nargiz & Mammadov, Jabir. New Key Exchange Protocol Based on Matrix Algebras. – 2023, 1-3. 10.1109/PCI60110.2023.10326004;

- Gasimov Vagif, Mammadzada Nargiz & Mammadov Jabir. New key exchange protocol based on matrix algebras // II International Conference on Information Security: Problems And Prospects, Baku, Azerbaijan, - 2022;

- Gasimov Vagif, Mammadzada Nargiz & Mammadov Jabir (2022). New symmetric encryption algorithm based on chaotic motion of molecules // II International Conference on Information Security: Problems and Prospects, Baku, Azerbaijan, – 2022;

- Gasimov Vagif, Mammadzada Nargiz. Data Shuffling Algorithm For Preserving Privacy and Utility Of Analysis, ITTA 2026 (3rd International Conference on Information Technologies and Their Applications), Azerbaijan

Dissertasiya işinin yerinə yetirildiyi təşkilatın adı. Dissertasiya işi Azərbaycan Texniki Universitetinin "Mühəndis riyaziyyatı və süni intellekt" kafedrasında yerinə yetirilmişdir.

Dissertasiyanın struktur bölmələrinin ayrılıqda həcmi qeyd olunmaqla dissertasiyanın işarə ilə ümumi həcmi. Dissertasiya işi 8527 işarədən ibarət girişdən, 29766 işarədən ibarət I fəsildən, 103406 işarədən ibarət II fəsildən, 61063 işarədən ibarət III fəsildən, 31341 işarədən ibarət IV fəsildən ibarət olmaqla ümumilikdə 259937 işarə ilə şərh olunmuşdur.

İŞİN QISA MƏZMUNU

Girişdə mövzunun aktuallığı əsaslandırılmış, tədqiqatın məqsədi, elmi yenilikləri və praktiki əhəmiyyəti şərh edilmişdir.

Birinci fəsildə *"Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində informasiya təhlükəsizliyi problemi"* – müasir informasiya texnologiyalarının tətbiqi şəraitində tibbi informasiya sistemlərinin (TİS) və xüsusi təyinatlı elektron sənəd dövriyyəsinin (ESDS) mövcud vəziyyəti, problemləri və inkişaf perspektivləri kompleks şəkildə təhlil edilmişdir.

Bu fəsildə ilkin olaraq **tibbi sənədlərin** spesifik xüsusiyyətləri araşdırılmışdır. Qeyd olunmuşdur ki, bu sənədlər fərdlərin sağlamlıq vəziyyəti, diaqnozları və genetik göstəriciləri haqqında kritik məlumatları ehtiva etdiyindən, onlara qarşı **konfidensiallıq**, **bütövlük** və **əlçatanlıq** (CIA triadası) tələbləri ən yüksək səviyyədə qoyulur. Tədqiqat zamanı məlumatların qorunmasını tənzimləyən beynəlxalq standartlar (ISO/IEC 27001, NIST 800-53) və hüquqi normativlər, xüsusilə **HIPAA** (Health Insurance Portability and

Accountability Act) və **GDPR** (General Data Protection Regulation) müddəaları dərindən analiz edilmiş, mövcud sistemlərin bu tələblərə uyğunluğu qiymətləndirilmişdir.

Tədqiqatın gedişində tibbi sistemlərə yönəlmiş **təhdid modelləri** təsnifləşdirilmişdir. Müəyyən edilmişdir ki, ənənəvi təhlükəsizlik mexanizmləri (məsələn, statik girişə nəzarət modelləri – DAC, MAC) dinamik dəyişən tibbi mühit (təcili yardım halları, filiallararası mübadilə) üçün çeviklik təmin edə bilmir. Eyni zamanda, mövcud standart şifrələmə alqoritmlərinin (RSA, AES) tətbiqi zamanı yaranan problemlər aşkar edilmişdir:

1. **Hesablama resurslarının səmərəsizliyi:** böyük həcmli tibbi təsvirlərin (DICOM standartlı MRT, KT görüntüləri) standart blok şifrələmə üsulları ilə emalı zamanı ciddi gecikmələr yaranır ki, bu da real zamanlı diaqnostika prosesinə mane olur.

2. **Açar idarəçiliyi problemləri:** Açıq kanallar üzərindən şifrələmə açarlarının təhlükəsiz ötürülməsi üçün istifadə olunan klassik protokollar (məsələn, Diffie-Hellman) gələcək kvant hesablamaları qarşısında potensial zəifliyə malikdir.

Bu problemlərin həlli istiqamətində **"Dərin müdafiə"** strategiyasının tətbiqi zərurəti əsaslandırılmışdır. Fəslin yekununda belə nəticə əldə olunmuşdur ki, tibbi verilənlərin yüksək səviyyəli mühafizəsini təmin etmək üçün **deterministik xaos nəzəriyyəsi**, **fraktal həndəsə**, **qeyri-standart matris cəbri** və **kombinator strukturlara (labirint nəzəriyyəsi)** əsaslanan yeni, hibrid kriptoqrafik metodların və paylanmış verilənlər bazası arxitekturalarının işlənib hazırlanması aktual elmi-texniki məsələdir. Bu yanaşma həm kriptoqrafik dayanıqlığı artırmağa, həm də sistemin performansını yüksəltməyə imkan verir.

İkinci fəsildə – *"Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində informasiyanın konfidensiallığının qorunması üsulları"* – dissertasiyanın əsas elmi-texniki nəticələri və təklif olunan alqoritmlər təsvir edilmişdir.

Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində informasiyanın konfidensiallığının qorunması üçün kriptoqrafik üsul və alqoritmlər bölməsində xüsusi təyinatlı, o cümlədən tibbi elektron sənəd dövriyyəsi sistemlərində (XTESDS) informasiyanın

konfidensiallığını təmin etmək üçün istifadə olunan müasir kriptoqrafik metodlar, onların təsnifatı, üstünlükləri və çatışmazlıqları geniş təhlil edilmişdir. Tədqiqat zamanı müəyyən edilmişdir ki, tibbi sənədlərin mühafizəsi üçün tətbiq olunan kriptoqrafik sistemlər iki əsas qrupa bölünür:

1. **Simmetrik şifrələmə sistemləri:** burada şifrələmə və deşifrələmə üçün eyni gizli açardan istifadə olunur (məsələn, DES, AES, 3DES). Bu metodlar yüksək sürətə malik olsa da, açarların tərəflər arasında təhlükəsiz paylanması (key distribution) problemini yaradır. Xüsusilə AES (Advanced Encryption Standard) standartı tibbi sistemlərdə geniş yayılsa da, böyük həcmli təsvirlərin (real-time video, yüksək keyfiyyətli MRT) emalı zamanı hesablama resurslarına qənaət baxımından bəzi məhdudiyyətlərə malikdir.

2. **Asimmetrik şifrələmə sistemləri:** burada bir-biri ilə riyazi əlaqəsi olan iki açardan (açıq və gizli) istifadə edilir (məsələn, RSA, ElGamal, Elliptik Əyrilər). Bu sistemlər açar paylanması problemini həll etsə də, hesablama mürəkkəbliyi simmetrik sistemlərdən qat-qat yüksəkdir və böyük verilənlərin birbaşa şifrələnməsi üçün əlverişli deyildir.

Yarımfəsildə həmçinin, son dövrlərdə aktuallaşan **axın şifrələməsi (stream ciphers)** və **blok şifrələməsi (block ciphers)** arasındakı fərqlər araşdırılmışdır. Tibbi sənədlərin xüsusiyyətləri (böyük həcm, yüksək korrelyasiya, real zamanlı ötürülmə tələbi) nəzərə alınaraq, axın şifrələməsinin bu sahə üçün daha perspektivli olduğu əsaslandırılmışdır.

Mövcud standartların təhlili göstərmişdir ki, "Əşyaların İnterneti" (IoT) və "Tibbi Əşyaların İnterneti" (IoMT) cihazlarının artması, eləcə də kvant hesablamalarının inkişafı fonunda klassik alqoritmlər gələcək təhdidlərə qarşı dayanıqsız ola bilər. Bu səbəbdən, dissertasiyada **deterministik xaos nəzəriyyəsinə** əsaslanan kriptoqrafik yanaşmaların tətbiqi zəruri hesab edilmişdir. Xaotik sistemlərin **erqodiklik**, **qarışdırma (mixing)** və **başlanğıc şərtlərə yüksək həssaslıq** kimi xüsusiyyətləri onların kriptoqrafik "qarışdırma" (confusion) və "yayılma" (diffusion) prinsiplərinə tam uyğun gəldiyini göstərir.

Nəticə etibarilə, bu yarımfəsildə əsaslandırılmışdır ki, xüsusi təyinatlı tibbi sistemlərdə yüksək təhlükəsizlik və sürəti təmin etmək üçün ənənəvi metodlarla yanaşı, **xaos nəzəriyyəsi**, **fraktal həndəsə** və **kombinator (labirint) strukturlara** əsaslanan yeni hibrid şifrələmə alqoritmlərinin işlənməsinə ehtiyac vardır. Bu təhlil dissertasiyanın sonrakı fəsillərində təklif olunan Broun hərəkəti, Labirint şifrələməsi və Matris protokollarının yaradılması üçün nəzəri baza rolunu oynamışdır.

Mətn tipli konfidensial informasiyanın qorunması üçün molekulların xaotik hərəkət modelinə əsaslanan şifrləmə üsulu. Bu yarımfəsildə müəllif tərəfindən mətn tipli tibbi sənədlərin (epikrizlər, rəylər, reseptlər) sürətli və təhlükəsiz şifrələnməsi üçün **molekulların Broun hərəkəti (Brownian motion)** fiziki modelinə əsaslanan yeni psevdo-təsadüfi ədədlər generatoru (PRNG) və axın şifrələmə (stream cipher) alqoritmi təklif edilmişdir. Broun hərəkəti mikroskopik hissəciklərin maye və ya qaz mühitində nizamsız, xaotik hərəkətidir. Bu prosesin riyazi modeli (Wiener prosesi) yüksək entropiyaya malikdir və proqnozlaşdırılması son dərəcə çətindir. Təklif olunan metodda qapalı $L \times W$ ölçülü fəzada molekulun hərəkəti simulyasiya edilir. Hər bir addımda molekulun yeni vəziyyəti (koordinat və sürət) aşağıdakı tənliklər sistemi ilə hesablanır:

$$V_{xi} = Round\left(\left(\left((V_{xi-1} \cdot (X_i + k)) \bmod M_{max}\right), r\right) + k\right)$$

$$T_i = Round\left(\left(\left((T_{i-1} \cdot k) \bmod (T + k)\right) \bmod X_{max}\right), r\right) + k$$

Burada, X_i, Y_i – molekulun toqquşma anındakı koordinatları; V_{xi}, V_{yi} – sürət vektorunun komponentləri; T_i – toqquşma anı (zaman); * k, r – sistemin xaosunu idarə edən gizli parametrlərdir (açarın bir hissəsi).

Generatorun iş prinsipi: 1. Başlanğıc şərtlər - açar kimi molekulun ilkin koordinatları (X_0, Y_0), ilkin sürəti (V_{x0}, V_{y0}) və mühit parametrləri daxil edilir. 2. Generasiya: hər toqquşma nöqtəsində alınan koordinatların kəsr hissələri (məsələn, vergüldən sonrakı 48 bit) götürülür və bit ardıcıllığına çevrilir. 3. Şifrələmə:

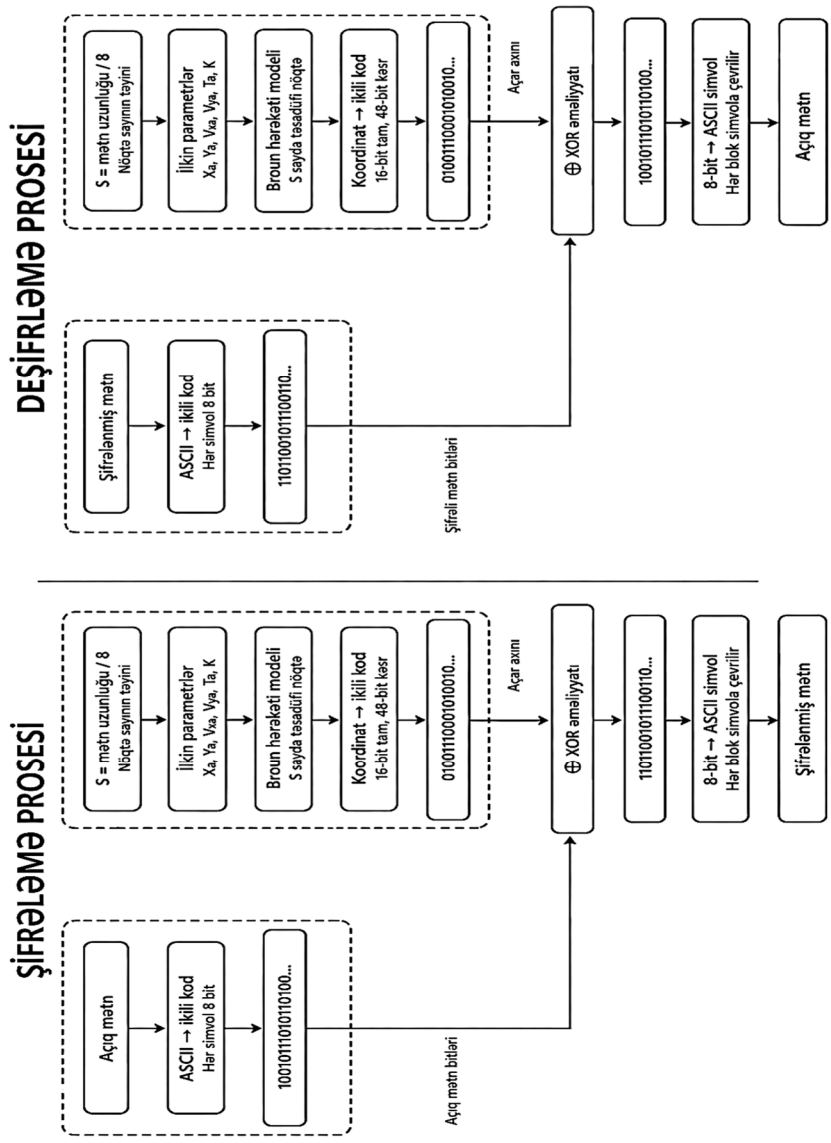
alınan psevdo-təsadüfi bit axını (Keystream) açıq mətnin bitləri ilə XOR ($\oplus$) əməliyyatına tabe tutulur: $C_i = P_i \oplus K_i$ [1, 8].

Bu metodun üstünlüyü onun **"kəpənək effekti"nə** malik olmasıdır: başlanğıc parametrlərdə 10^{-15} tərtibində kiçik bir dəyişiklik tamamilə fərqli açar axını yaradır. NIST testləri bu generatorun çıxışlarının statistik təsadüfilik tələblərinə tam cavab verdiyini göstərmişdir (şəkil 1). Axın şifrəsinin təhlükəsizliyi dinamik uzunluqlu gizli açarların gözlənilməzliyindən asılıdır. Yaradılan ardıcıllıqların psevdo-təsadüfiliyini qiymətləndirmək üçün bir sıra standart testlər tətbiq edilmişdir.

Xi-kvadrat testinin nəticələrinə görə D statistikası orta hesabla 15–17 diapazonunda olmuş, α=0,05 səviyyəsində qəbul edilən 16,9 həddinə uyğundur. NIST monobitlər üçün 9 testindən isə P dəyərləri 0,04–0,5 arasında alınmışdır ki, bu da P≥0,01 şərtini ödəyərək ardıcıllığın təsadüfi olduğunu təsdiqləyir. Açar həssaslığı testində isə açarın bir bitinin dəyişdirilməsi ilə deşifrə zamanı tamamilə fərqli nəticələr əldə edilmiş, şifrənin açara yüksək həssaslığı göstərilmişdir.

Beləliklə, Broun hərəkəti modelinə əsaslanan təklif olunan psevdo-təsadüfi ədədlər generatoru statistik testlər və açar həssaslığı analizi ilə təsdiqlənmişdir. Molekulun trayektoriyasının başlanğıc şərtlərə yüksək həssaslığı proqnozlaşdırılması çətin açar axınının formalaşmasını təmin edir. Nəticələr göstərir ki, təbii fiziki proseslərin xaotik dinamikasına əsaslanan bu yanaşma axın şifrələmə sistemlərinin təhlükəsizliyinin artırılması üçün perspektivli bir həll təqdim edir.

Tibbi diaqnostikada istifadə olunan rəqəmsal təsvirlər (Rentgen, MRT, KT, USM) adi mətn fayllarından fərqli olaraq, piksellər arasında yüksək korrelyasiya (əlaqəlilik) əmsalına malikdir. Yəni, qonşu piksellərin rəng dəyərləri bir-birinə çox yaxın olur ki, bu da vizual strukturun adi şifrələmə üsulları (məsələn, ECB rejimli blok şifrələr) ilə tam gizlədilməməsinə gətirib çıxarır. Bu problemin həlli üçün dissertasiyada **dərinliyə doğru axtarış (DFS - Depth First Search)** alqoritmi ilə generasiya edilən təsadüfi labirint strukturuna və **Xaos nəzəriyyəsinə** əsaslanan yeni hibrid şifrələmə metodu işlənilmişdir.



Şəkil 1. Şifrləmə və deşifrləmə alqoritmlərinin sxematik təsviri

Təklif olunan metodun iş prinsipi **"Qarışdırma-Yayma"** arxitekturasına əsaslanır və aşağıdakı mərhələlərdən ibarətdir:

1. Xaotik labirintin generasiyası: İlkin olaraq, şifrələnəcək təsvirin ölçüsünə ($N \times M$) uyğun ölçüdə virtual bir tor (grid) yaradılır. Labirintin başlanğıc koordinatları (x_0, y_0) və hərəkət istiqamətlərinin seçimi **Feigenbaum logistik xəritəsi** vasitəsilə idarə olunur:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

Burada $r \in [3.57,4]$ xaos parametrdir. Bu tənlik vasitəsilə alınan psevdo-təsadüfi ədədlər DFS alqoritminin "qonşu xana seçimi" funksiyasında istifadə edilir. Nəticədə, bütün xanaları ziyarət edən, lakin dövrəsi olmayan, təkrarlanmaz struktura malik bir labirint (örtən ağac)formalaşdırılır (şəkil 2).

0	18	17	16	21	24	25	26	27	28	29	355	319	318	317	316	356	357	358	359
1	19	20	15	22	23	399	35	34	31	30	354	320	313	314	315	382	383	384	360
2	3	4	13	12	38	37	36	33	32	325	322	321	312	311	310	364	363	362	361
156	157	5	14	11	39	40	41	331	330	324	323	304	305	385	309	365	366	286	285
155	154	6	9	10	167	166	42	332	329	326	353	303	306	307	308	367	288	287	284
152	153	7	8	164	163	165	43	333	328	327	301	302	371	370	369	368	289	282	283
151	158	159	160	161	162	168	44	334	339	338	300	373	372	377	378	381	290	281	390
150	147	146	175	174	173	169	45	335	336	337	299	374	375	376	379	380	291	280	279
149	148	145	129	128	171	170	46	47	352	340	298	297	296	295	294	293	292	277	278
142	143	144	130	127	172	50	49	48	351	341	342	232	233	234	386	387	275	276	391
134	133	132	131	126	125	51	350	349	348	344	343	231	236	235	389	388	274	273	392
135	120	121	122	123	124	52	55	56	347	345	346	230	229	237	240	241	272	393	393
136	119	118	180	181	176	53	54	57	58	225	226	227	228	238	239	242	271	394	270
137	138	117	179	178	177	64	63	60	59	224	218	217	210	209	208	245	246	270	269
140	139	116	182	183	66	65	62	61	223	222	219	216	211	212	207	248	247	395	268
141	114	115	101	100	67	68	69	71	221	220	215	214	213	206	249	249	266	267	267
112	113	103	102	99	90	85	86	87	72	73	74	202	203	204	205	250	264	263	262
111	184	104	97	98	91	84	89	88	77	76	75	201	199	198	197	251	252	396	261
110	106	105	96	93	92	83	82	81	78	398	190	191	200	195	196	254	253	259	260
109	107	108	95	94	185	186	187	80	79	188	189	192	193	194	256	255	257	258	397

Şəkil 2. Permutasiya matrisi

2. Permutasiya (yerdəyişmə) matrisinin qurulması: Labirintin yaradılması zamanı alqoritmin hərəkət trayektoriyası qeydə alınır. Bu trayektoriya əsasında unikal indekslərdən ibarət M **(Path Matrix)** matrisi formalaşdırılır. M matrisinin hər bir elementi (m_{ij}) təsvirin piksellərinin yeni yerini təyin edir. Təsvirin pikselləri bu ardıcıllıqla yenidən düzüldükdə, təsvirin vizual strukturu tamamilə dağılır və piksellər arasında fəza əlaqəsi (spatial correlation) qırılır.

3. Diffuziya və stek yaddaşı uzunluğu: Yalnız yerdəyişmə kifayət etmədiyi üçün (çünki rəng dəyərləri (histogram) dəyişmir) diffuziya prosesi tətbiq edilir. Bu məqsədlə DFS alqoritminin işləməsi zamanı istifadə olunan **Stek** yaddaşının dinamik dəyişən dərinliyi istifadə olunur. Hər bir (i, j) xanası üçün stekdə olan elementlərin sayı hesablanır və S- stek uzunluğu matrisi yaradılır (şəkil 3). Şifrələmə prosesi aşağıdakı XOR əməliyyatı ilə həyata keçirilir:

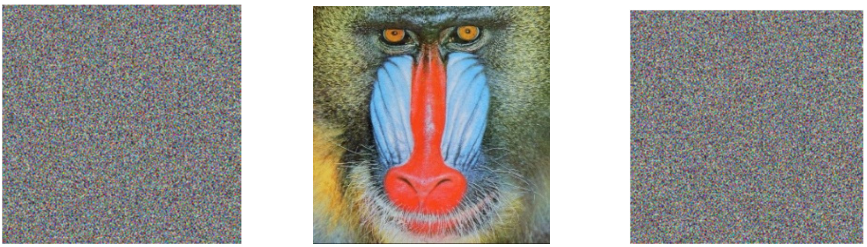
$$C_i = P_{perm(i)} \oplus S_i \oplus K_{stream}.$$

Burada, C_i – şifrələnmiş pikselin dəyəri; $P_{perm(i)}$ – yeri dəyişdirilmiş (permutasiya olunmuş) piksel; S_i – Stek uzunluğu (bu dəyər labirintin strukturundan asılı olaraq təsadüfi dəyişir); K_{stream} – xaotik generatorla yaradılmış əlavə açar axınıdır.

0	17	16	15	16	19	20	21	22	23	24	207	202	201	200	199	200	201	202	203
1	18	19	14	17	18	33	30	29	26	25	206	203	196	197	198	209	210	211	204
2	3	4	13	12	33	32	31	28	27	208	205	204	195	194	193	208	207	206	205
139	140	5	14	11	34	35	36	213	212	207	206	187	188	195	192	209	210	169	168
138	137	6	9	10	145	144	37	214	211	208	209	186	189	190	191	210	171	170	167
135	136	7	8	143	142	143	38	215	210	209	184	185	214	213	212	211	172	165	166
134	137	138	139	140	141	144	39	216	221	220	183	216	215	220	221	224	173	164	163
133	130	129	150	149	148	145	40	217	218	219	182	217	218	219	222	223	174	163	162
132	131	128	119	118	147	146	41	42	229	220	181	180	179	178	177	176	175	160	161
125	126	127	120	117	148	45	44	43	228	221	222	117	118	119	178	179	158	159	162
124	123	122	121	116	115	46	229	228	227	224	223	116	121	120	181	180	157	156	163
125	110	111	112	113	114	47	50	51	226	225	226	115	114	121	124	125	126	155	164
126	109	108	119	120	115	48	49	52	53	110	111	112	113	122	123	128	127	154	165
127	128	107	118	117	116	59	58	55	54	109	104	103	96	95	94	129	130	153	166
130	129	106	119	120	61	60	57	56	109	108	105	102	97	98	93	132	131	154	151
131	104	105	92	91	62	63	64	65	66	107	106	101	100	99	92	133	148	149	150
102	103	94	93	90	81	80	81	82	67	68	69	88	89	90	91	134	147	146	145
101	104	95	88	89	82	79	84	83	72	71	70	87	86	85	84	135	136	147	144
100	97	96	87	84	83	78	77	76	73	78	77	78	87	82	83	138	137	142	143
99	98	99	86	85	86	87	88	75	74	75	76	79	80	81	140	139	140	141	144

Şəkil 3. Stek yaddaş əsasında yaradımış XOR qiymətlər cədvəli

4. İterativ gücləndirmə: Alqoritm "uçqun effekti"ni (avalanche effect) artırmaq üçün bir neçə raund (məsələn, 5 dövr) təkrarlanır. Nəticədə alınan şifrələnmiş təsvirin histoqramı tamamilə bərabər paylanmış (uniform) formaya düşür, piksellər arası korrelyasiya əmsalı isə 0-a yaxınlaşır (məsələn: horizontal – 0.0021, vertikal – 0.0018). Bu göstəricilər metodun statistik və diferensial hücumlara qarşı yüksək dayanıqlığını sübut edir (şəkil 4).



a) b) c)

Şəkil 4. a) açar ilə şifrələnmiş təsvir (K1=8763572198561905), b) düzgün açar ilə deşifrələnmiş təsvir (K1=8763572198561905), c) yanlış açar ilə deşifrələnmiş təsvir (K1=8763572198561805)

Təhlükəsizlik və keyfiyyət analizi. Təklif olunan alqoritmin effektivliyi genişmiqyaslı eksperimentlərlə yoxlanılmışdır:

1. Histoqram analizi. Orijinal tibbi təsvirlərin histoqramı (rənglərin paylanma tezliyi) qeyri-bərabər olduğu halda, Labirint şifrləmə ilə şifrlənmiş təsvirlərin histoqramı tamamilə bərabər paylanmış (uniform) formaya düşür. Bu, şifrəli təsvirin orijinal məzmun haqqında heç bir statistik məlumat sızdırmadığını və statistik hücumlara qarşı dayanıqlı olduğunu göstərir (şəkil 5, şəkil 6).

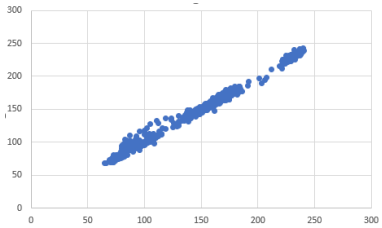
2. Korrelyasiya analizi. Orijinal təsvirdə qonşu piksellər arasında korrelyasiya əmsalı vahidə yaxındır ($R \approx 0.95 - 0.98$). Təklif olunan alqoritm tətbiq edildikdən sonra bu göstərici kəskin şəkildə azalaraq 0-a yaxınlaşmışdır (horizontal: 0.0021, vertikal: 0.0018, diaqonal: 0.0034). Bu, piksellər arasındakı əlaqənin tamamilə qırıldığını və vizual strukturun yox olduğunu təsdiqləyir (şəkil 7).

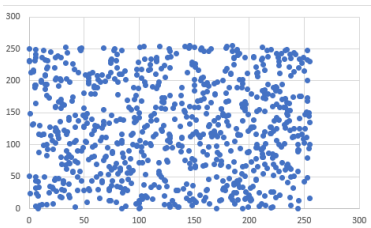
a) b) c)

Şəkil 5. Orijinal şəkillərin histoqram analizi: a) qırmızı, b) yaşıl, c) mavi

a) b) c)

Şəkil 6. Şifrlənmiş şəkillərin histoqram analizi: a) qırmızı, b) yaşıl, c) mavi





a) b)

Şəkil 7. Təsvirlərin üfüqi qonşu piksellərinin korrelyasiya asılılığı qrafiki: a) orijinal, b) şifrələnmiş (eyni nəticə vertikal və diaqonal piksellər üçün də əldə edilmişdir)

NIST testləri ilə analiz. Təklif edilən alqoritmin statistik göstəriciləri NIST testləri vasitəsilə də yoxlanılmışdır. Bu məqsədlə 7 testdən istifadə edilmiş və müxtəlif ölçülü şifr-təsvirlər üzərində təcrübələr aparılmış, bütün yoxlamaların nəticələri müsbət olmuşdur (cədvəl).

Cədvəl. NIST testlərinin nəticələri

Test	Nəticə
Tezlik (monobit) testi	P - dəyər = 0.799
Blok daxilində tezlik testi	P - dəyər = 0.569
Blokdakı ən uzun tək ədədlər üçün test	P - dəyər = 0.151
Kumulyativ cəmlər testi	P - irəli dəyər = 0.900 P - tərs dəyər = 0.674
İcra testi	P - dəyər = 0.998
İkili matris Rank testi	P - dəyər = 0.381
Təxmini entropiya testi	P - dəyər = 0.303

3. Entropiya analizi. Şifrələnmiş təsvirin informasiya entropiyası hesablanmış və nəticə **7.999** (maksimum mümkün dəyər 8-dir) alınmışdır. Bu, məlumatın tamamilə xaotik olduğunu və təsadüfi səs-küydən fərqlənmədiyini göstərir.

4. Açar həssaslığı. Açarda (məsələn, r parametrində və ya başlanğıc koordinatda) 10^{-15} tərtibində kiçik bir dəyişiklik edildikdə, şifrələnmiş təsvirdə piksellərin 50%-dən çoxu dəyişir. Bu xüsusiyyət alqoritmin diferensial hücumlara qarşı yüksək dayanıqlığını təmin edir.

Məhsuldarlıq. Alqoritm böyük həcmli tibbi görüntülərin şifrələnməsində standart asimmetrik alqoritmlərdən (RSA) dəfələrlə sürətli işləyir və real zamanlı sistemlərdə tətbiq üçün əlverişlidir.

Nəticə. Labirint şifrləmə metodu tibbi təsvirlərin konfidensiallığını təmin etmək üçün həm riyazi (xaos, qraf nəzəriyyəsi), həm də statistik baxımdan güclü bir həll yoludur. Alqoritm vizual məlumatı tamamilə tanınmaz hala gətirir və açar olmadan orijinalın bərpası nəzəri cəhətdən qeyri-mümkündür [2].

Klassik Diffie-Hellman protokoluna alternativ olaraq, **tərsi tapılmayan (determinantı sıfır olan) matrislər** üzərində qurulmuş yeni asimmetrik protokol işlənilmişdir. Protokolun iş prinsipi: 1. Tərəflər (Alice və Bob) ortaq, determinantı sıfır olan ($det(C) = 0$) bir C matrisi seçirlər. 2. Alisa gizli A matrisini və q qüvvətini, Bob isə gizli B matrisini və p qüvvətini seçir. 3. Alisa $S_A = A \cdot C^q$, Bob isə $S_B = C^p \cdot B$ matrislərini hesablayıb bir-birinə göndərirlər. 4. Tərəflər aldıqları natamam açarları öz gizli parametrləri ilə tamamlayırlar. Yekun ortaq açar: $S = A \cdot C^{q+p} \cdot B$. Üçüncü tərəf açıq kanalda S_A və S_B-ni əldə etsə belə, C matrisinin tərsi olmadığı üçün tənliyi həll edib A və B gizli matrislərini bərpa edə bilmir. Bu, protokolun xətti cəbr hücumlarına qarşı dayanıqlığını təmin edir. Protokolun dayanıqlığı aşağıdakı hücum ssenariləri üzrə analiz edilmişdir:

- **Xətti cəbr hücumlarına qarşı dayanıqlıq.** Hücumçu açıq kanaldan C, S_{A1} və S_{B1} matrislərini əldə edir. Məqsəd gizli A və ya B matrislərini tapmaqdır. Lakin $S_{A1} = A \cdot C^q$ tənliyində C matrisi **tərsi tapılmayan** olduğu üçün bu tənliklər sistemi **natamam təyin**

olunmuş sistemə çevrilir. Yəni, tənliklərin sayı məchulların sayından azdır və sonsuz sayda A matrisi bu tənliyi ödəyə bilər. Hücumçu həqiqi A matrisini unikal şəkildə müəyyən edə bilmir. Əlavə olaraq, ikinci raundda daxil edilən M və N matrisləri tənliklər sisteminin mürəkkəbliyini daha da artırır və trivial həlləri istisna edir.

- **Açar fəzası və "Qaba qüvvə" analizi.** Protokolun sındırılması üçün tələb olunan resurslar açar fəzasının (mümkün matrislərin sayı) böyüklüyü ilə ölçülür. Dissertasiyada aparılan kombinator hesablamalar göstərir ki, elementləri $[0,1000]$ aralığında olan sadəcə 4×4 ölçülü matrislər üçün belə tərsi tapılmayan matrislərin sayı təxminən 10^{60} tərtibindədir. Bu, 200-bitlik şifrələmə açarına ekvivalentdir və müasir superkompüterlər üçün belə "külli axtarış" (brute-force) metodunu qeyri-mümkün edir. Matrisin ölçüsü (n) artdıqca, təhlükəsizlik səviyyəsi eksponensial olaraq artır.
- **Ortadakı adam hücumu.** Təklif olunan protokol rəqəmsal imzalar və ya sertifikatlarla birlikdə istifadə edildikdə, M və N matrislərinin yalnız tərəflərə məlum olması hesabına aktiv dinləmə hücumlarına qarşı dayanıqlılıq nümayiş etdirir.

Protokolun işləmə sürəti klassik alqoritmlərlə müqayisə edilmişdir. Diffie-Hellman protokolunda istifadə olunan **modulyar eksponentasiya** əməliyyatı böyük ədədlər üçün (məsələn, 2048 bit) ciddi hesablama resursu tələb edir. Təklif olunan metodda isə əsas əməliyyat **matrislərin vurulmasıdır**. Matris vurma əməliyyatı müasir prosessorlarda (CPU/GPU) yüksək səviyyədə paralelləşdirilə bilir. Aparılan eksperimentlər (Intel Core i5, 8GB RAM mühitində) göstərmişdir ki, açarın generasiyası və mübadiləsi prosesi 100×100 ölçülü matrislər üçün belə 0.23 saniyədən az vaxt tələb edir. Eyni təhlükəsizlik səviyyəsində matris əsaslı protokol, ənənəvi RSA və DH alqoritmlərindən təxminən 3-5 dəfə daha sürətli nəticə göstərmişdir.

Bu xüsusiyyətlər təklif olunan protokolun hesablama resursları məhdud olan mühitlərdə (IoT tibbi sensorlar, mobil terminallar) və real zamanlı sistemlərdə tətbiqi üçün yüksək potensiala malik olduğunu sübut edir [3, 7, 9-10].

Səhiyyə sistemlərində toplanan böyük həcmli verilənlərin ("Big Data") elmi-tədqiqat və statistika məqsədilə analizi zamanı fərdi məlumatların (pasiyentlərin kimliyi) gizliliyi təmin edilməlidir. Lakin ənənəvi tam təsadüfi qarışdırma metodları (məsələn, Fisher-Yates shuffle) verilənlərin strukturunu tamamilə dağıdır və bu da onların analitik faydalılığını azaldır. Dissertasiyada bu problemi həll etmək üçün **Labirint qarışdırma** adlı yeni, yerli təsadüfilik prinsipinə əsaslanan anonimləşdirmə alqoritmi işlənilmişdir.

Bu metodun əsas məqsədi verilənləri elə qarışdırmaqdır ki, fərdi qeydlərin re-identifikasiyası (yenidən tanınması) mümkün olmasın, lakin verilənlər bazasının ümumi statistik xüsusiyyətləri (lokal klasterlər, paylanma qanunauyğunluqları) qorunub saxlanılsın.

Alqoritmin iş prinsipi: 1. **Verilənlərin məkan təsviri:** 1D (bir ölçülü) verilənlər massivi (məsələn, pasiyent siyahısı) 2D (iki ölçülü) virtual matrisə və ya labirintə ($N \times N$) transformasiya edilir. 2. **Labirint trayektoriyası:** DFS alqoritmi ilə təsadüfi bir yol (path) yaradılır. Verilənlərin yerdəyişməsi bu yol boyunca həyata keçirilir. 3. **Tənbəl gəzinti mexanizmi:** Alqoritmin əsas yeniliyi **"Tənbəl Gəzinti"** modelinin tətbiqidir. Hər bir iterasiyada (t) elementin qonşu xana ilə yerini dəyişməsi ehtimalı (p_{swap}) ilə yanaşı, yerində qalma ehtimalı (p_{lazy}) da nəzərə alınır. Əgər $Rand_{val} < p_{lazy} \rightarrow$ element yerində qalır, əgər $Rand_{val} \geq p_{lazy} \rightarrow$ element labirintdəki qonşusu ilə yerini dəyişir. Bu yanaşma sistemin **aperiodik** olmasını təmin edir və Markov zənciri nəzəriyyəsinə əsasən, iterasiyaların sayı artdıqca sistemin stabil qarışma vəziyyətinə yaxınlaşmasına zəmanət verir.

Riyazi əsaslandırma. Dissertasiyada sübut edilmişdir ki, Labirint qarışdırma alqoritminin yaratdığı keçid matrisi (K) **primitivdir** (irreducible və aperiodic). Perron-Frobenius teoreminə əsasən, bu o deməkdir ki, iterasiya sayı (t) artdıqca, verilənlərin paylanması eksponensial sürətlə bərabər paylanmaya (uniform distribution) yaxınlaşır. Məxfilik riski (R_t) aşağıdakı kimi qiymətləndirilir:

$$R_t = \| K^t - J \| \leq (\sigma_2(K))^t.$$

Burada $\sigma_2(K)$ keçid matrisinin ikinci ən böyük sinqulyar dəyəridir (< 1). Bu düstur göstərir ki, iterasiyalar artdıqca fərdi məlumatın ilkin mövqeyi ilə əlaqəsi (re-identifikasiya riski) eksponensial olaraq sıfıra yaxınlaşır.

Nəticə. Labirint qarışdırma alqoritmi "Fisher-Yates" (tam xaos) və "Blok-Qarışdırma" zəif qarışdırma metodları arasında optimal balansı təmin edir. O, məlumatları kifayət qədər qarışdıraraq **k-anonimlik** və **l-müxtəliflik** prinsiplərini dəstəkləyir, eyni zamanda verilənlərin lokallıq xüsusiyyətini qoruyaraq tibbi analizlər (məsələn, xəstəliklərin coğrafi yayılması və ya yaş qrupları üzrə klasterləşmə) üçün faydalı olaraq qalır. Bu metod xüsusilə böyük həcmli tibbi verilənlərin bulud mühitində emalı və tədqiqatçılarla paylaşılması zamanı təhlükəsizliyi təmin etmək üçün idealdır [12].

Üçüncü fəsildə *"Xüsusi təyinatlı elektron sənəd dövriyyəsi sistemlərində informasiya təhlükəsizliyinin təmin edilməsinin təşkilati və texniki aspektləri"* mövzusuna həsr edilmiş dissertasiya işinin bu fəslində təklif olunan kriptoqrafik metodların və protokolların real tibbi informasiya sistemlərində (TİS) tətbiqi üçün zəruri olan sistem arxitekturası, verilənlər bazasının paylanmış strukturu və girişə nəzarət mexanizmləri işlənib hazırlanmışdır.

Tədqiqat zamanı müəyyən edilmişdir ki, müasir tibb müəssisələri (xəstəxanalar, poliklinikalar, laboratoriyalar) adətən mərkəzi ofis və coğrafi baxımdan səpələnmiş filiallardan ibarət mürəkkəb struktura malikdir. Belə sistemlərdə məlumatların mərkəzləşdirilmiş qaydada saxlanması "Vahid Uğursuzluq Nöqtəsi" (Single Point of Failure - SPOF) riskini yaradır və şəbəkə qopmaları zamanı filialların işini iflic edir. Bu problemin həlli üçün dissertasiyada **hibrid paylanmış arxitektura** təklif edilmişdir. Bu modeldə hər bir filial öz lokal verilənlər bazasına sahibdir, lakin eyni zamanda mərkəzi serverlə (bulud və ya data mərkəzi) sinxronizasiya olunur.

Təhlükəsizlik modelinin əsas komponentləri aşağıdakılardır:

Elektron imza infrastrukturu. Tibbi sənədlərin (reseptlər, epikrizlər) bütövlüyünü və inkaredilməzliyini təmin etmək üçün təkmilləşdirilmiş elektron imza sxemi tətbiq olunur. Bu sxemdə

sənədin heş-funksiyası (məsələn, SHA-256) hesablanır və müəllifin gizli açarı ilə şifrələnir.

Dinamik rollar və icazələr. Tibbi personalın (həkim, baş həkim, laborant, qeydiyyatçı) sistemdəki səlahiyyətlərini idarə etmək üçün dinamik RBAC modeli işlənilmişdir. Bu modeldə istifadəçiyə statik rollarla yanaşı, vəziyyətdən asılı olaraq (məsələn, növbətçi həkim rejimi, fövqəladə hal) müvəqqəti icazələr verilə və ya geri alına bilər [5].

Tibb müəssisələrinin fasiləsiz işini təmin etmək üçün dissertasiyada **liderisiz replikasiya** modelinə əsaslanan paylanmış verilənlər bazası arxitekturası təklif edilmişdir. Ənənəvi Lider-İzləyici arxitekturasından fərqli olaraq, bu modeldə hər bir filial (qovşaq) həm oxuma, həm də yazma əməliyyatlarını müstəqil icra edə bilər.

Təklif olunan arxitekturanın iş prinsipi: 1. **Lokal yazma:** Həkim sənədi filialın lokal bazasına yazır (offline rejimdə belə işləyir). 2. **Asinxron replikasiya:** Şəbəkə əlaqəsi bərpa olunduqda və ya dövri olaraq, lokal dəyişikliklər digər filiallara və mərkəzi bazaya ötürülür. 3. **Fraqmentasiya:** Məlumatlar həm üfüqi (filiallara görə pasiyent qrupları), həm də şaquli (məlumatın növünə görə - mətn, təsvir) fraqmentasiya prinsipləri əsasında paylanır ki, bu da sorğuların sürətini artırır.

Liderisiz sistemlərin ən böyük problemi eyni vaxtda müxtəlif qovşaqlarda eyni sənəd üzərində dəyişiklik edilməsi zamanı yaranan **konfliktlərdir**. Məsələn, A filialındakı həkim pasiyentin diaqnozunu dəyişir, eyni anda B filialındakı laborant həmin pasiyentin analiz nəticələrini əlavə edir. Dissertasiyada bu problemin həlli üçün **"Tranzaksiya cədvəli"** və **zaman damğası** əsaslı yeni sinxronizasiya alqoritmi işlənmişdir:

- **Versiya vektorları.** Hər bir sənəd üçün versiya vektoru saxlanılır. Dəyişiklik zamanı vektor artırılır.
- **Tranzaksiya cədvəli.** Hər bir qovşaqda icra olunan tranzaksiyaların statusunu (icra olundu/gözləyir) saxlayan xüsusi cədvəl yaradılır.

• **Konfliktin həlli:** İki qovşaq arasında verilənlərin birləşdirilməsi zamanı, obyektlərin ID-ləri üzrə hash strukturlu çoxluqlar yaradılır:

$$Tr_{conflicts} = HashSet_{by_{ObjectID}}\left(\sum Tr_i^A + \sum Tr_j^B\right).$$

Sistem konfliktli obyektlər üçün zaman damğalarına baxır. "Sonuncu yazan qazanır" prinsipi və ya semantik birləşdirmə (əgər dəyişikliklər fərqli sahələrdədirsə) tətbiq edilərək ən aktual versiya bütün bazalara yayılır, digəri isə geri qaytarılır(rollback).

Bu yanaşma sistemin **CAP teoreminə** uyğun olaraq, yüksək əlçatanlıq) və bölünməyə dözümlülük nümayiş etdirməsini təmin edir [6].

Dördüncü fəsildə *"Xüsusi təyinatlı müəssisələrdə informasiyanın konfidensiallığının qorunması üsul və alqoritmlərinin proqram həlləri və tətbiqi"* adlı dissertasiyada təklif olunan nəzəri metodların və alqoritmlərin proqram səviyyəsində realizasiyası, onların işləmə prinsipləri, alınan nəticələrin statistik analizi və mövcud standartlarla müqayisəsi verilmişdir. İşlənmiş kriptoqrafik metodlar **C#** proqramlaşdırma dilində, *Microsoft Visual Studio* mühitində realizasiya edilmişdir. Yaradılan proqram kompleksi aşağıdakı funksional modullardan ibarətdir:

Mətn şifrləmə modulu. Molekulların Broun hərəkəti modelinə əsaslanan, istifadəçi tərəfindən daxil edilən başlanğıc parametrlərə (koordinat, sürət) uyğun psevdo-təsadüfi ədədlər generasiya edərək mətn tipli sənədlərin (TXT, DOCX) bit səviyyəsində XOR əməliyyatı ilə şifrələnməsi və deşifrələnməsi.

Təsvir şifrləmə modulu. Başlanğıc dəyərlər ilə Feygembaun və DFS metodu ilə labirint genasiyasi və bu generasiyadan yaranan iki matris vasitəsi ilə yerdəyişmə və dəyər dəyişmə üsulları vasitəsi ilə təsvir fayllarının (BMP, JPG,) DFS labirint alqoritmi vasitəsilə şifrələnməsi. İstifadəçi interfeysində şifrələmə prosesi, labirintin vizual görüntüsü və şifrələnmiş təsvirin ("səs-küy" şəkli) nəticəsi əks olunur.

Labirint qarışdırma modulu. Cədvəl strukturlu verilənlərin DFS vasitəsi ilə generasiya edilmiş matris ilə anonimliyinin və faydalılığının qorunması üçün csv tipli sənədlərdə Python proqram təminatı ilə qarışdırma üsulunun tədbiqi.

Açar mübadiləsi modulu: Matris cəbrinə əsaslanan protokolun simulyasiyası. Burada tərəflər arasında matrislərin generasiyası, hasillərin hesablanması və ortaq açarın əldə edilməsi prosesi Python dilində avtomatlaşdırılmışdır.

Alınmış nəticələrin təhlili və tövsiyələrin işlənməsi

Dissertasiyada təklif edilmiş metod və alqoritmlərin üstünlükləri və əlverişli istifadə sahələri aşağıdakı kimi təhlil edilmişdir:

- **Təsadüfilik mənbəyinin unikallığı.** Metod, psevdo-təsadüfi ədədlər generatoru (PRNG) üçün fiziki bir prosesdən (molekulların xaotik hərəkəti, simulyasiya olunsa belə) ilhamlanır. Bu, sırf riyazi funksiyalara əsaslanan ənənəvi xaotik PRNG-lərdən fərqli bir yanaşmadır və yeni növ təsadüfilik mənbəyi təklif edir.
- **Xaotik xüsusiyyətlərdən istifadə.** Broun hərəkətinin özündə olan xaotik təbiət, yəni başlanğıc şərtlərə qarşı yüksək həssaslıq və proqnozlaşdırıla bilməmə kriptoanalizə qarşı dayanıqlığı artırmaq üçün əsasdır. Açarda (başlanğıc koordinatlar, sürətlər, k əmsalı) edilən kiçik bir dəyişiklik tamamilə fərqli bir psevdo-təsadüfi ədədlər ardıcıllığı (şifrələmə axını) yaradır.

Təklif edilən alqoritm ümumiyyətlə axın sifrələmə metodu olduğu üçün axın şifrələmənin tətbiq olunduğu sahələrdə geniş istifadə edilə bilər. Bu xüsusiyyətləri onu aşağıdakı sahələrdə əlverişli edir:

1. **Real zamanlı kommunikasiya.** Məlumatın davamlı bir axın şəklində gəldiyi və aşağı gecikmənin vacib olduğu sistemlər.
2. **Məhdud resurslu mühitlər.** Aşağı hesablama gücü, yaddaş və ya enerji sərfiyyatına malik cihazlar.
3. **Yüksək sürətli məlumat ötürülməsi.**
4. **Xəta yayılmasının minimuma endirilməsi lazım olan hallar.**
5. **Proqram təminatı implementasiyasının asanlığı.**

İstifadə sahələrinə əsasən ümumiləşdirmək olar:

- **Hərbi və müdafiə strukturları:** real zamanlı, təhlükəsiz rabitənin təmin edilməsi kritikdir.
- **Kəşfiyyat və əks-kəşfiyyat agentlikləri:** məxfi əlaqə kanallarının qurulması, əməliyyat məlumatlarının real zamanda ötürülməsi.
- **Hüquq mühafizə orqanları və fövqəladə hallar xidmətləri:** əməliyyat zamanı təhlükəsiz və fasiləsiz səsli məlumat rabitəsinin təmin edilməsi.
- **Diplomatik korpus və xarici işlər nazirlikləri:** ölkə daxilindəki mərkəzlə xaricdəki səfirliklər və konsulluqlar arasında məxfi məlumatların təhlükəsiz ötürülməsi.

Şəkil formatlı sənədlərin şifrələnməsi üçün təklif edilən labirint əsaslı təsvir şifrələmə metodu, xüsusilə təsvir kriptoqrafiyası sahəsinə və ümumi təhlükəsizliyə aşağıdakı potensial töhfələri və üstünlükləri təqdim edir:

- **Təsvir xüsusiyyətlərinin nəzərə alınması:** metod birbaşa təsvirlərin şifrələnməsi üçün nəzərdə tutulmuşdur.
- **İkiqat kriptoqrafik mexanizm:** metod iki əsas addımdan ibarətdir: piksel qarışdırılması və piksel dəyərlərinin dəyişdirilməsi.
- **Xaotik və təsadüfi proseslərin kombinasiyası.** Labirintin generasiyası üçün açar kimi Feygenbaumun xaotik funksiyasından (PRNG üçün) və DFS alqoritminin təsadüfi seçimlərindən istifadə edilir.
- **Təhlükəsizlik analizi ilə təsdiqlənmə.** İşdə aparılan təhlillər metodun statistik hücumlara və diferensial analizə qarşı analizlərdən dayanıqlı olduğunu göstərir.
- **Təkrar əməliyyatlarla gücləndirmə.** Qarışdırma və dəyişdirmə addımlarının ən azı 5 dəfə təkrarlanması, diffuziya və konfuziya prinsiplərinin təsirini artıraraq kriptoanalizə qarşı müqaviməti gücləndirməyə xidmət edir.

Qarışdırma ilə anonimləşdirmənin müsbət tərəfləri:

- Statistik xüsusiyyətlərin qorunması (sütun səviyyəsində).
- Konseptual sadəlik.
- Tətbiqin asanlığı.
- Əlaqənin qırılması: qarışdırılmanın fərqli sütunlardakı dəyərlər arasında eyni sətirdə (yazıda) olan birbaşa əlaqəni qırır.
- Məlumat itkisinin az olması (sütun analizi üçün).

Matris əsaslı açar mübadilə protokolunun potensial üstünlükləri:

- **Fərqli riyazi əsas:** protokol, faktorizasiya və diskret loqarifmdən fərqli bir riyazi problemə əsaslanır.
- **Potensial performans üstünlükləri (spesifik hallarda):** matris əməliyyatları müasir prosessorlarda və ya xüsusi aparat təminatında çox səmərəli şəkildə həyata keçirilə bilər.

Ümumi olaraq hər bir elektron sənəd dövriyyəsi sistemlərində informasiya texnologiyalarının infrastrukturunun təhlükəsizliyi üçün önəmli olan bir çox məqamlar vardır ki, hər bir müasir İT korporativ mühitində tətbiq olunmalı və nəzərə alınmalıdır. Bu önəmli məqamlar aşağıda göstərilmişdir:

- kompüterdə istifadə edilən tətbiqlərin hər zaman yeni versiyalara yenilənməsi vacibdir.
- elektron poçta daxil olan şübhəli əməlləri açmamaq.
- antivirus proqramlarından istifadə.
- VPN protokolları ilə hər bir əlaqə gizli kanal ilə reallaşdırılmalıdır.
- sistemə daxil olan hər bir istifadəçinin şifrəsinin təhlükəsizliyinin təminində parollar üçün tələb olunan şərtlərin yerinə yetirilməsi vacibdir.
- iki faktorlu authentifikasiyanın istifadə edilməsi.
- sistemdən istifadə edən hər bir istifadəçi şübhəli olan saytlara və yaxud linklərə daxil olmamağı barədə məlumatlandırılmalıdır.
- Proqramçılar sistemə daxil olan sorğularda SQL injeksiyanın qarşısını almaq üçün sorğuda iştirak edən hər bir parametr üçün validasiyalar ilə qadağalar qoymalıdır. Web tətbiqlər üzərində

olan sistem əlavələri üçün isə nəzərə alınmalı təhlükələrdən digəri isə CSRF hücumlarıdır.

- sistemdən istifadə edən hər bir istifadəçinin parolları bazalarda açıq şəkildə saxlanılmamalıdır.
- buffer yaddaşın aşması. Bunun həllində daxil edilən dataların validasiyası və ya aşma zamanı xəta xəbərinin verilməsi vacibdir.
- servis rəddi. Belə halların qarşısının alınması üçün server tərəfindən kənar sorğular ayırd edilərək serverin çökməsinin qarşısı alınmalıdır.
- qırıla bilən giriş idarəetməsi: Bu çatışmazlığın həllində hər bir istifadəçiyə səlahiyyətlər doğru şəkildə, yeni ən az səlahiyyət prinsipi ilə yaradılmalı və qaynaqlara müraciətlər daha sərt şərtlər ilə yoxlanılaraq icazələr verilməlidir.

Yekun olaraq, dissertasiyada aparılan sınaqlar və müqayisəli analizlər təklif olunan metodların tibbi informasiya sistemlərində tətbiqinin həm təhlükəsizlik, həm də performans baxımından səmərəli olduğunu təsdiqləmişdir.

ƏSAS NƏTİCƏLƏR

1. Xaotik proseslərin tətbiqi ilə kriptoqrafik sistemlərin gücləndirilməsi. Tədqiqatda xaotik proseslərin təsadüfə oxşar və proqnozlaşdırılması çətin olan təbiətindən istifadə edilərək kriptoqrafik metodların təhlükəsizliyi artırılmışdır. Bu yanaşma, xüsusilə açar generasiyası və şifrələmə proseslərində dinamik və mürəkkəb strukturlar yaradaraq mövcud alqoritmlərin zəifliklərini aradan qaldırmağa imkan vermiş, kriptoqrafik tətbiqlər üçün daha etibarlı və xarici hücumlara qarşı davamlı bir təməl formalaşdırmışdır.

2. Mətn formatlı sənədlər üçün yeni axın şifrələmə alqoritmi. Elmi yenilik olaraq, mətn tipli tibbi məlumatların şifrələnməsi üçün molekulların xaotik Broun hərəkəti modelinə əsaslanan təsadüfi ədədlər generatoru ilə işləyən yeni axın şifrələmə alqoritmi yaradılmışdır. Bu alqoritm, generasiya edilən təsadüfi bitlər

ardıcıllığını mətnin bitləri ilə birləşdirərək hər bir simvol üçün unikal şifrələmə tətbiq edir. Təklif olunan metod yüksək sürətli şifrələməni təmin etməklə yanaşı, statistik analizlərə qarşı da yüksək müqavimət göstərir.

3. Təsvir formatlı məlumatlar üçün labirint əsaslı şifrələmə. Tibbi təsvirlərin məzmununun effektiv şəkildə qorunması məqsədilə Dərinliyə Doğru Axtarış (DFS) alqoritmi ilə generasiya edilən labirintlərdən istifadə edən yeni bir şifrələmə metodu işlənmişdir. Bu metod, təsvirin piksellərini labirintin yolları boyunca qarışdıraraq onların orijinal mövqelərini bərpa etməyi olduqca mürəkkəbləşdirir, təsvirlərin vizual məlumatını tamamilə tanınmaz hala gətirir və açar olmadan orijinal təsvirin bərpası prosesini nəzəri cəhətdən mümkünsüz edir.

4. Matris cəbrinə əsaslanan açar mübadiləsi protokolu. Şəbəkələrdə məlumat ötürülməsi zamanı tərəflər arasında təhlükəsiz açar mübadiləsini təmin etmək üçün matris cəbrinin birtərəfli funksiyalarına (tərsi tapılmayan matrislər) əsaslanan yeni bir protokol hazırlanmışdır. Bu protokol, tərəflərin açıq kanallar vasitəsilə ümumi bir məxfi açar əldə etməsinə imkan yaradır və tərsinə hesablanması çətin olan matris əməliyyatları sayəsində gizliliyi təmin edir.

5. Verilənlərin anonimləşdirilməsi üçün yeni alqoritm. Analitik məqsədlər üçün məlumatların istifadəsi zamanı fərdi məxfiliyin qorunmasını təmin etmək məqsədilə labirint generasiyasından əldə edilən qarışdırma matrisinə əsaslanan bir anonimləşdirmə alqoritmi yaradılmışdır. Bu alqoritm, verilənlər bazasındakı həssas məlumatları geri çevrilməsi mümkün olmayan şəkildə qarışdıraraq onların kimliyini gizlədir və analitiklərə fərdi məxfiliyi pozmadan məlumatlar üzərində təhlillər aparmağa imkan verir.

6. Paylanmış verilənlər bazaları üçün sinxronizasiya və replikasiya arxitekturası. Paylanmış tibbi sistemlərdə verilənlərin bütövlüyünü və konsistentliyini təmin etmək məqsədilə tranzaksiyalar cədvəlinə əsaslanan yeni bir sinxronlaşdırma və replikasiya arxitekturası işlənmişdir. Bu model, bazanın müxtəlif nüsxələrində aparılan bütün əməliyyatları xüsusi bir cədvəldə qeydə

alaraq dəyişikliklərin nizamlı şəkildə digər nüsxələrə ötürülməsini təmin edir, məlumat itkisinin və ziddiyyətlərin qarşısını alır.

7. Sənədlərin təhlükəsiz ötürülməsi üçün qorunan kanalların yaradılması. Sənədlərin uzaq məsafədə yerləşən verilənlər bazalarına təhlükəsiz şəkildə ötürülməsi üçün etibarlı kommunikasiya kanallarının yaradılması metodu təklif edilmişdir. Bu metod, ötürülən məlumatları güclü şifrələmə alqoritmləri ilə qoruyur və tunelləmə texnologiyalarından istifadə edərək məlumatların kənar müdaxilələrdən təcrid olunmasını təmin edir.

8. Resurslara müraciət üçün dinamik audentifikasiya və avtorizasiya modelləri. İnformasiya sistemlərində resurslara girişə nəzarəti təmin etmək üçün dinamik rollar və icazələr sisteminə əsaslanan audentifikasiya və avtorizasiya modeli hazırlanmışdır. Bu model, istifadəçilərin kimliyini yoxlamaqla yanaşı, onların sistemdəki rollarına uyğun olaraq hansı məlumatlara və funksiyalara giriş edə biləcəyini müəyyən edir. Təklif olunan dinamik yanaşma rolların və icazələrin real zaman rejimində idarə olunmasına imkan verərək təhlükəsizliyi və idarəetmə çevikliyini artırır.

Dissertasiya işinin əsas nəticələri aşağıdakı elmi əsərlərdə dərc edilmişdir:

1. Gasimov, V.A., Mammadov, J.I., Mammadzada, N.F. Stream encryption method based on the chaotic brownıan motion model of molecules // 4th International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2022). 3-4 November, http://icidca.com/2022/. – Coimbatore, India. Procedia Computer Science, vol.215, – 2022, – pp. 577-588.
2. Gasimov, V.A. Maze based image encryption method constructed by random number generation / V.A.Gasimov, N.F.Mammadzada, J.I.Mammadov [et al.] // Eurasian Journal of Mathematical and Computer Applications. ISSN 2306-6172. Vol. 12, Issue 3, – 2024, – pp.35-50. (Web of Sciences).

3. Gasimov, V.A., Mammadzada, N.F., Mammadov, J.I. New Key Exchange Protocol Based on Matrix Algebras // 5th International Conference on Problems of Cybernetics and Informatics (PCI), Azerbaijan, – Baku, – 2023, – pp. 1-3, doi: 10.1109/PCI60110.2023.10326004.
4. Gasimov, V.A., Mammadov, J.I., Mammadzada, N.F. Method of hidden transmission of information based on fractals and its software // Tomsk State University, Journal of Control and Computer Science, – Russian Federation. – 2023(65), – pp.95-104. DOI: doi: 10.17223/19988605/65/10
5. Gasimov, V.A., Mammadzada, N.F., Mammadov, J.I, Aliyeva, K.J. The problem of information protection in electronic document management systems of medical organizations // Problems of Informatization and Management. – 2025, – pp.37-45. 10.18372/2073-4751.81.20127.
6. Gasimov, V.A., Mammadzada, N.F. Architecture and model of a special-purpose electronic document management system with a distributed structure // Mathematics and Computer Science, – 2024, vol. 8, no.2, – pp. 120-129.
7. Gasimov, V.A., Mammadzada, N.F., Mammadov, J.I. Matris əsaslı yeni açar mübadiləsi protokolu // II International Conference on Informatıon Security: Problems and Prospects, – Baku, – 2022.
8. Gasimov, V.A., Mammadzada, N.F., Mammadov, J.I. Molekulların xaotik hərəkətinə əsaslan yeni simmetrik şifrələmə alqoritmi // II International Conference on Informatıon Securıty: Problems and Prospects, – Baku, – 2022.
9. Gasimov, V.A., Mammadzada, N.F., Mammadov, J.I. // Investıgatıon Of The Securıty Of A Key Exchange Protocol Based on Matrıx Algebra // Mathematics and Computer Science, – 2024, vol. 8, no. 2, – pp.101-104.
10. Mammadzada, N.F. Matrıx Based Key Exchange Protocol // Proceedıngs of the 8th International Conference on Control And Optimization With Industrial Applıcations. – Baku, – 2022.

11. Gasimov Vagif, Mammadzada Nargiz. Data Shuffling Algorithm For Preserving Privacy and Utility Of Analysis, ITTA 2026 (3rd International Conference on Information Technologies and Their Applications), Azerbaijan
12. Gasimov A. Vagif, Mammadzada F. Nargiz, Mustafayeva A. Esmira, Aliyeva J. Kamala, Probabilistic stochastic shuffling for privacy-preserving data analytics with maintained analytical utility and robust statistical performance, Advanced Mathematical Models & Applications (çap mərhələsindədir).

Dissertasiyanın müdafiəsi 30 iyun 2026-cı il tarixində saat 14:00-da Azərbaycan Dövlət Neft və Sənaye Universitetinin nəzdində fəaliyyət göstərən FD 2.48 Dissertasiya Şurasının iclasında keçiriləcək.

Ünvan: AZ1010, Bakı şəhəri, Azadlıq prospekti 20, Azərbaycan Dövlət Neft və Sənaye Universiteti.
E-mail: info@asoiu.edu.az

Dissertasiya işi ilə Azərbaycan Dövlət Neft və Sənaye Universitetinin kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Azərbaycan Dövlət Neft və Sənaye Universitetinin rəsmi internet saytında yerləşdirilmişdir.

Avtoreferat 27 May 2026-cı il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb: 26.05.2026

Kağızın formatı: A5

Həcm: 39859

Tiraj: 100