UOT: 336.004

Leyla Nadir qızı İBADOVA
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəçilik Akademiyası magistrantı
E-mail: leilaibadova594@gmail.com,

Pərviz Əhməd oğlu QURBANOV
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəçilik Akademiyası
“Dövlət idarəçiliyində informasiya texnologiyaları” kafedrasının dosenti,
iqtisad üzrə fəlsəfə doktoru
E-mail: parviz.gurban@gmail.com
https://doi.org/10.30546/4.71.73001.2025.003.014

MALİYYƏDƏ SİMMETRİK ŞİFRƏLƏMƏNİN TƏTBİQLƏRİ

Xülasə

Tədqiqatın əsas məqsədi - simmetrik şifrələmənin təhlükəsizlik baxımından üstünlüklərini müəyyənləşdirmək, simmetrik şifrələmənin maliyyə sahəsindəki tətbiqinin səmərəliliyini , maliyyə qurumları və istifadəçilər üçün faydalarını qiymətləndirmək, onun maliyyə rabitəsində necə tətbiq olunduğunun əsas aspektlərini araşdırmaqdır.

Tədqiqatın metodologiyası olaraq açarların idarə edilməsi metodları, təhlükəsizlik analizləri, standartlar və qanunvericiliyə uyğunluq metodları tətbiq edilmişdir. Bu metodlar simmetrik şifrələmənin maliyyə sahəsində tətbiqinin effektivliyini artırmaq və onu daha da inkişaf etdirmək üçün müxtəlif yanaşmalar irəli sürür.

Tədqiqatın əhəmiyyəti çoxşaxəlidir. Tədqiqat, daha güclü şifrələmə metodlarının inkişafını stimullaşdıracaq. Tədqiqat nəticəsində əldə olunan məlumatlar, banklar və digər maliyyə qurumlarının müştəri məlumatlarını qorumaq üçün daha müasir və etibarlı metodlardan istifadə etmələrinə kömək edə bilər.Bu isə öz növbəsində iqtisadiyyatın ümumi səmərəliliyinə müsbət təsir göstərəcək.

Tədqiqatın nəticəsi - Simmetrik şifrələmə maliyyə xidmətlərində məlumatların təhlükəsizliyi və məxfiliyini qorumaqda mühüm rol oynayır. Açarların təhlükəsiz idarə olunması və paylaşılması məsələləri hələ də əsas məsələ olaraq qalır. Bu tədqiqat, şifrələmə alqoritmlərinin maliyyə sistemlərində daha təhlükəsiz və səmərəli tətbiqi üçün təkmilləşdirilmiş metodlar və protokolların inkişaf etdirilməsi zərurətini vurğulayır.

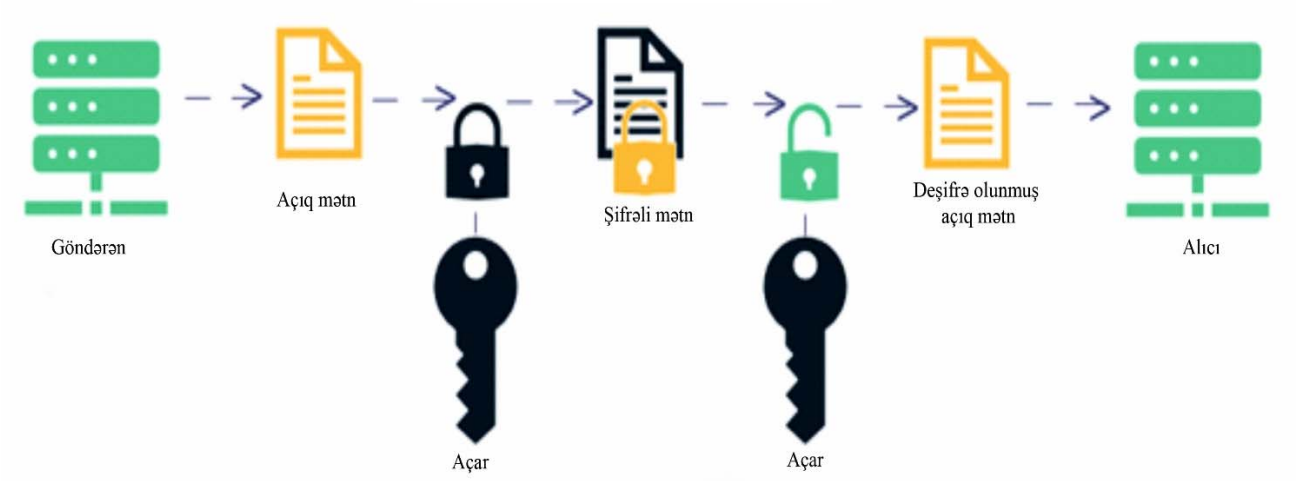
Tədqiqatın orijinallığı və elmi yeniliyi - Mövcud şifrələmə alqoritmlərinin üstünlüklərini və zəifliklərini nəzərə alaraq yeni metodların inkişaf etdirilməsini və qiymətləndirilməsini stimullaşdırır. Açarların idarə edilməsi və saxlanması məsələləri şifrələmənin effektivliyinə təsir edən vacib amillərdən biridir. Bu sahədə yeni metodların inkişafı tədqiqatın əsas elmi yeniliklərindən ola bilər.

Açar sözlər: Simmetrik şifrələmə, maliyyə, onlayn bankçılıq, ödəniş sistemləri, maliyyə məlumat bazaları, maliyyə kommunikasiyası, kibertəhlükəsizlik, açar idarəetmə.

Giriş

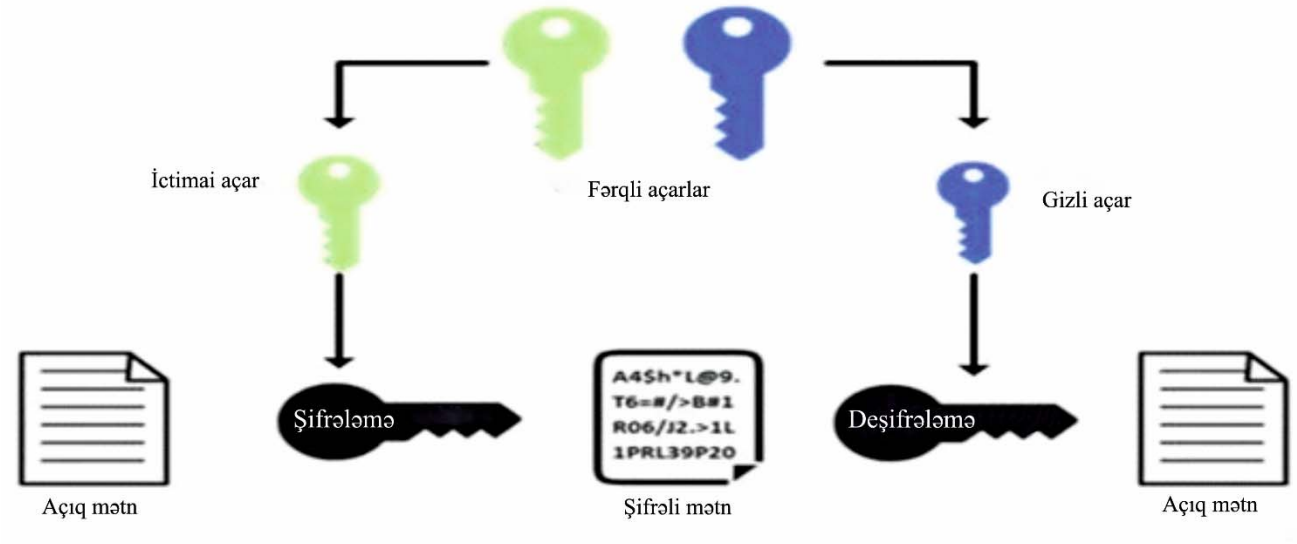
Simmetrik şifrələmə elektron məlumatları həm şifrələmək, həm də deşifrə etmək üçün yalnız bir açarın (gizli açar) istifadə edildiyi şifrələmə növüdür. Simmetrik şifrələmə vasitəsilə əlaqə quran qurumlar açarı mübadilə etməlidirlər ki, həmin açar şifrənin açılması prosesində istifadə olunsun. Bu şifrələmə üsulu mesajları şifrələmək və deşifrə etmək üçün bir cüt açarın - biri ictimai, digəri gizli istifadə edildiyi asimmetrik şifrələmədən fərqlənir.[1]

Simmetrik şifrələmə



Şəkil 1. Simmetrik şifrələmənin işləmə prinsipi

Asimmetrik şifrələmə



Şəkil 2. Asimmetrik şifrələmənin işləmə prinsipi

Simmetrik şifrləmə alqoritmlərindən istifadə edərək məlumatın "şifrlənməsində" məqsəd bundan ibarətdir ki, şifrələnmiş mətni açmaq üçün istifadə olunan gizli açarı olmayan heç kəs tərəfindən məlumat başa düşülməsin. Açara sahib olan nəzərdə tutulan alıcı mesaja sahib olduqdan sonra alqoritm öz hərəkətini tərsinə çevirir ki, mesaj orijinal oxuna bilən formasına qaytarılsın.

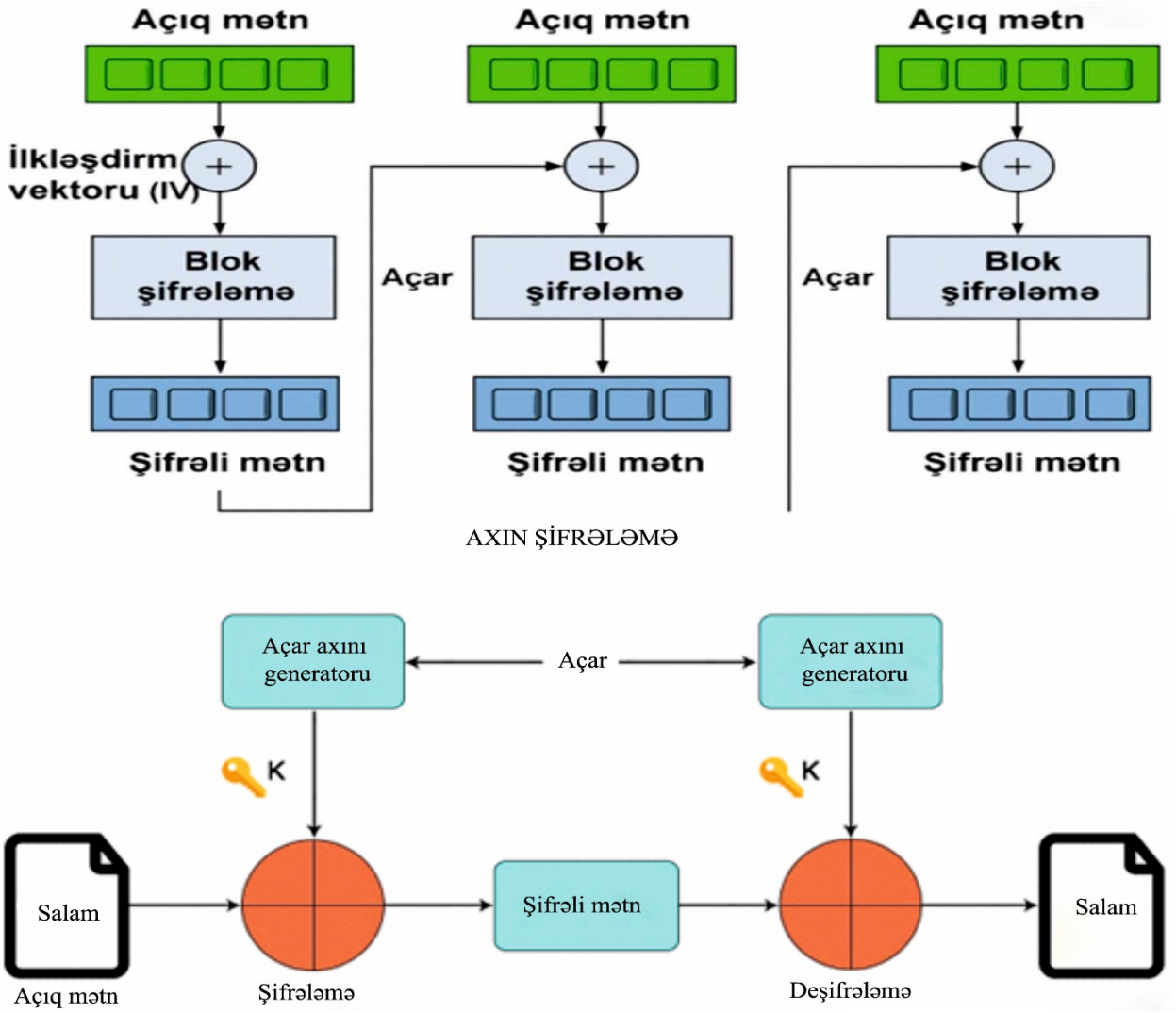
Göndərən və alıcının hər ikisinin istifadə etdiyi məxfi açar xüsusi parol/kod ola bilər və ya təhlükəsiz təsadüfi nömrə generatoru (RNG) tərəfindən yaradılan təsadüfi hərf və ya rəqəmlər silsiləsi ola bilər. Bank səviyyəli şifrələmə üçün simmetrik açarlar FIPS 140-2 kimi sənaye standartlarına uyğun sertifikatlaşdırılmış RNG istifadə edərək yaradılmalıdır. [2]

Simmetrik şifrələmə alqoritmlərinin iki növü var:

1. Blok alqoritmləri. Blok şifrələmədə şifrələmə vahidi kimi blokdan (qeyd olunmuş bitlər ardıcıllığı) istifadə edilir ki, o da eyni uzunluqda olan şifrələnmiş mətn blokuna çevrilir.

2. Axın alqoritmləri. Məlumat sistem yaddaşında saxlanılmaq əvəzinə axın zamanı şifrələnir. [3, səh 71-72]

Blok şifrələmə



Şəkil 4. Axın alqoritmi

Bugünkü kiber-dünyada məlumatların bütün formalarına icazəsiz giriş riski həmişə mövcuddur. Ən çox risk altında olan maliyyə və ödəniş sistemi məlumatlarıdır ki, bu da müştərilərin şəxsiyyətini müəyyənləşdirən məlumatları (PII) və ya ödəniş kartı detallarını ifşa edə bilər. Şifrələmə PII-ni qorumaq və ödəniş əməliyyatlarını emal edən müəssisələrin hər gün, hər dəqiqə qarşılaşdığı riskləri azaltmaq üçün vacibdir. [1]

Simmetrik şifrələmənin onlayn bank əməliyyatlarında tətbiqi

Simmetrik şifrələmə onlayn bank əməliyyatlarının təhlükəsizliyinin təmin edilməsində mühüm rol oynayır. Onlayn bankçılıq təhlükəsiz kommunikasiya kanallarına və istifadəçi etimadnamələri, maliyyə əməliyyatları və şəxsi məlumatlar kimi həssas məlumatların qorunmasına əsaslanır. Bu təhlükəsizlik problemlərini müxtəlif yollarla həll etmək üçün simmetrik şifrələmə istifadə olunur: [4]

Məlumat məxfiliyi. Simmetrik şifrələmə istifadəçinin cihazı (məsələn, kompüter və ya mobil cihaz) və bankın serverləri arasında ötürülən məlumatların şifrələnməsi üçün istifadə olunur. Bu, icazəsiz şəxslər məlumatları ələ keçirsələr belə, şifrələnmə zamanı istifadə olunan açar olmadan onu başa düşə və ya manipulyasiya edə bilməmələrini təmin edir. [4]

Təhlükəsiz giriş və doğrulama. Simmetrik şifrələmə istifadəçinin onlayn bank hesabına daxil olmaq üçün istifadə etdiyi məlumatlarını (istifadəçi adı və şifrə) qorumaq üçün tətbiq olunur. Məlumat ötürmə zamanı şifrələnir, bu da icazəsiz şəxslərin rabitəni kəsə bilsələr belə,lazımlı məlumat

əldə etmələrini olduqca çətinləşdirir. [5]

Tranzaksiya təhlükəsizliyi. Maliyyə əməliyyatları, o cümlədən fond köçürmələri və hesab ödənişləri, həssas məlumatların mübadiləsini nəzərdə tutur. Simmetrik şifrələmə bu əməliyyatların məxfiliyini və bütövlüyünü təmin edir. Məbləğ və alıcı kimi əməliyyatın təfərrüatları ötürülməzdən əvvəl şifrələnir. [6]

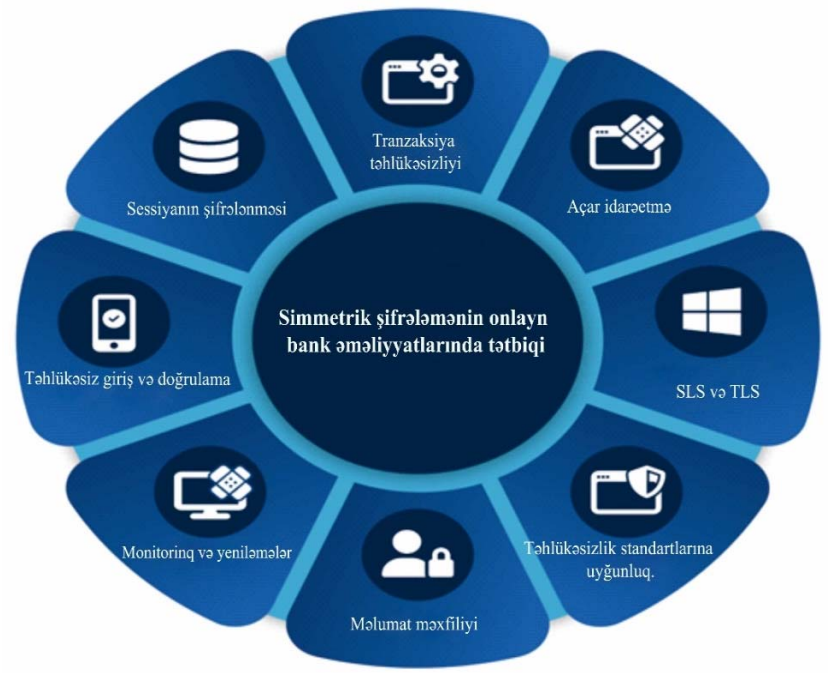
Sessiyanın şifrələnməsi. Onlayn bank seansları simmetrik şifrələmə ilə təmin edilir. İstifadəçi daxil olduqdan sonra təhlükəsiz seans qurulur və həmin sessiya zamanı mübadilə edilən məlumatları şifrələmək üçün simmetrik açarlar yaradılır. Bu, icazəsiz şəxslərin istifadəçi ilə bank serveri arasındakı əlaqəni dinləməsinin qarşısını alır. [7]

Secure Sockets Layer (SSL) və Transport Layer Security (TLS). SSL və onun varisi TLS onlayn ünsiyyəti təmin etmək üçün geniş istifadə olunan protokollardır. Onlar simmetrik şifrələmə alqoritmlərindən istifadə edərək istifadəçinin brauzeri ilə bankın serveri arasında mübadilə edilən məlumatları şifrələyir. Bu şifrələmə ötürülən məlumatın məxfiliyini və bütövlüyünü təmin edir. [4]

Açar idarəetmə. Simmetrik şifrələmə şifrələmə açarlarının təhlükəsiz idarə edilməsini tələb edir. Onlayn bank sistemləri şifrələmə açarlarını icazəsiz girişdən qorumaq üçün etibarlı açar idarəetmə təcrübələrini həyata keçirir. Buraya açarların təhlükəsiz yaradılması, paylanması və saxlanması daxildir. [7]

Təhlükəsizlik standartlarına uyğunluq. Onlayn bankçılıqda simmetrik şifrələmə Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) və digər regional və ya milli məlumatların mühafizəsi qanunları kimi təhlükəsizlik standartlarına və qaydalarına uyğun olmalıdır. Uyğunluq onlayn bank sisteminin müəyyən edilmiş təhlükəsizlik tələblərinə cavab verməsini təmin edir. [5]

Davamlı monitorinq və yeniləmələr. Onlayn bankçılıq sistemləri potensial təhlükəsizlik təhdidlərini aşkar etmək və onlara cavab vermək üçün davamlı monitorinqdən keçir. Ortaya çıxan zəiflikləri aradan qaldırmaq və sistemin ümumi təhlükəsizliyini artırmaq üçün şifrələmə protokolları və alqoritmlərinin müntəzəm yenilənməsi həyata keçirilir. [4]



Şəkil 5. Simmetrik şifrələmənin onlayn bank əməliyyatlarında tətbiqi sxemi

Simmetrik şifrələmənin maliyyə kommunikasiyasında tətbiqi

Simmetrik şifrələmə maliyyə rabitəsinin təmin edilməsində, maliyyə institutları, müəssisələr və fiziki şəxslər arasında mübadilə edilən həssas məlumatların məxfiliyinin və bütövlüyünün

təmin edilməsində mühüm rol oynayır. Simmetrik şifrələmənin maliyyə rabitəsində necə tətbiq olunduğunun əsas aspektləri bunlardır:

Məlumatların məxfiliyi. Simmetrik şifrələmə əməliyyat təfərrüatları, hesab məlumatları və digər həssas məlumatlar daxil olmaqla, maliyyə mesajlarının məzmununu şifrələmək üçün istifadə olunur. Bu şifrələmə rabitə ələ keçirilsə belə, şifrə açma açarı olmadan məlumatın oxunmaz qalmasını təmin edir. [1]

Rabitə üçün təhlükəsiz protokollar. Maliyyə institutları tez-tez veb-əsaslı ünsiyyət üçün HTTPS (Hypertext Transfer Protocol Secure) kimi təhlükəsiz rabitə protokollarından və digər məlumat mübadiləsi növləri üçün təhlükəsiz fayl ötürmə protokollarından istifadə edirlər. Bu protokollar tranzit zamanı məlumatları qorumaq üçün simmetrik şifrələmədən istifadə edir. [5]

Mesaj şifrələmə. Elektron məlumat mübadiləsi (EDI), SWIFT (Society for Worldwide Interbank Financial Telecommunication) və ya digər rabitə kanalları vasitəsilə ötürülən maliyyə mesajları adətən simmetrik şifrələmə alqoritmlərindən istifadə etməklə şifrələnir. Bu, əməliyyat təfərrüatlarının məxfiliyini qoruyur və icazəsiz girişin qarşısını alır. [8]

Doğrulama və bütünlük. Simmetrik şifrələmə məlumatların autentifikasiyası mexanizmlərini təmin etməklə maliyyə kommunikasiyasının bütövlüyünü təmin etməyə kömək edir. Rəqəmsal imzalar və mesajın identifikasiyası kodları (MAC) simmetrik şifrələmə ilə yanaşı göndəricinin həqiqiliyini yoxlamaq və ötürülən məlumatların hər hansı saxtakarlığını və ya dəyişdirilməsini aşkar etmək üçün istifadə olunur. [3]

Əsas idarəetmə təcrübələri. Simmetrik şifrələmədə effektiv açar idarəçiliyi çox vacibdir. Maliyyə institutları şifrələmə açarlarının yalnız səlahiyyətli tərəflər arasında paylaşılmasını təmin etmək üçün təhlükəsiz açar paylanması və idarəetmə təcrübələrindən istifadə edir. Açarların müntəzəm olaraq yenilənməsi və güclü,təsadüfi yaradılan açarların istifadəsi rabitənin təhlükəsizliyini artırır. [7]

Virtual şəxsi şəbəkələr (VPN). Maliyyə ünsiyyətində, xüsusən də uzaqdan bağlantılar və təşkilatlararası əlaqə üçün VPN-lərdən tez-tez istifadə olunur. Simmetrik şifrələmə VPN tunelləri daxilində məlumatların təhlükəsizliyini təmin edir, ictimai internet üzərində təhlükəsiz və özəl rabitə kanalı yaradır. [9]

Qaydalara uyğunluq. Maliyyə institutları məlumat təhlükəsizliyi və məxfiliyi ilə bağlı müxtəlif qaydalara və standartlara əməl etməlidir. Simmetrik şifrələmə həssas maliyyə məlumatlarının qorunması üçün möhkəm və standartlaşdırılmış metod təqdim etməklə bu uyğunluq tələblərinə cavab verdiyini göstərir. [4]

Təhlükəsiz məlumat saxlama. Maliyyə institutları çoxlu sayda əməliyyat və müştəri məlumatlarını saxlayır. Bu saxlanılan məlumatların təhlükəsizliyini təmin etmək üçün simmetrik şifrələmə tətbiq edilir və nəticədə fiziki təhlükəsizlik pozulsa belə, məlumatın icazəsiz girişdən qorunmasını təmin edir. [5]

Davamlı monitorinq və insidentlərə cavab. Maliyyə təşkilatları potensial təhlükəsizlik təhdidlərini aşkar etmək və onlara cavab vermək üçün davamlı monitorinq və insidentlərə cavab mexanizmləri tətbiq edir. Bura şübhəli fəaliyyətlərin monitorinqi, nümunələrin təhlili və hər hansı təhlükəsizlik insidentlərinin operativ şəkildə həlli daxildir. [4]

Nəticə

Məqalə maliyyə əməliyyatlarının təmin edilməsində və həssas məlumatların qorunmasında simmetrik şifrələmənin əsas rolunu, simmetrik şifrələmənin onlayn bankçılıqda infrastrukturun əsas elementi olduğunu ümumiləşdirməklə yekunlaşır. O, maliyyə sektorunda inkişaf edən kibertəhlükəsizlik təhdidlərini həll etmək üçün davamlı innovasiya və əməkdaşlığa ehtiyac olduğunu vurğulayır.

ƏDƏBİYYAT

1. https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
2. Selected articles on Key Management (2012-today) by Ashiq JA, Dawn M. Turner, Guillaume Forget, James H. Reinholm, Peter Landrock, Peter Smirnoff, Rob Stubbs, Stefan Hansen and more.
3. Əliquliyev R.M., İmamverdiyev Y.N.. Kriptoqrafiyanın əsasları, Bakı 2006, səh 71-72.
4. Uma Dixit.Cryptography — Security in E-Banking. IOSR Journal of Business and Management (IOSR-JBM).
5. Kewin Chikomo, Ming Ki Chong, Alpan Arnab, Andrew Hutchison, "Security of Mobile Banking".
6. https://www.linkedin.com/advice/3/how-can-you-secure-financial-transactions#how-does-cryptography-secure-financial-transactions
7. Simmetrik Açar Şifrələmə - bankçılıqda niyə, harada və necə istifadə olunur (2019), Peter Smirnoff & Dawn M. Turner.
8. https://www.devglan.com/online-tools/text-encryption-decryption
9. https://openvpn.net/solutions/industries/finance/

Лейла Надир кызы Ибадова
E-mail: leilaibadova594@gmail.com,

Парвиз Ахмад оглы Гурбанов
Академия государственного управления при Президенте Азербайджанской Республики
доцент кафедры "Информационные технологии в государственном управлении"
доктор философии по экономике
E-mail: parviz.gurban@gmail.com

Применение симметричного шифрования в финансах

Резюме

Основная цель исследования — определить преимущества симметричного шифрования с точки зрения безопасности, оценить эффективность его применения в финансовом секторе, выгоды для финансовых учреждений и пользователей, а также рассмотреть основные аспекты его применения в финансовых коммуникациях.

В качестве **методологии исследования** применялись ключевые методы управления, анализ безопасности, стандарты и методы соблюдения законодательства. Эти методы предлагают различные подходы к повышению эффективности применения симметричного шифрования в финансовой сфере и его дальнейшему развитию.

Значимость исследования многогранна. Исследование будет стимулировать разработку более надежных методов шифрования. Полученная в результате исследования информация может помочь банкам и другим финансовым учреждениям использовать более современные и надежные методы защиты данных клиентов. Это, в свою очередь, окажет положительное влияние на общую эффективность экономики.

Результаты исследования: Симметричное шифрование играет важную роль в защите безопасности данных и конфиденциальности в финансовых услугах. Вопросы безопасного управления ключами и их совместного использования по-прежнему остаются серьезной проблемой. В этом исследовании подчеркивается необходимость разработки усовершенствованных методов и протоколов для более безопасной и эффективной реализации алгорит-

мов шифрования в финансовых системах.

Оригинальность и научная новизна исследования: Стимулирует разработку и оценку новых методов с учетом преимуществ и недостатков существующих алгоритмов шифрования. Вопросы управления и хранения ключей являются одними из важных факторов, влияющих на эффективность шифрования. Разработка новых методов в этой области может стать одним из главных научных новшеств исследования.

Ключевые слова: Симметричное шифрование, финансы, онлайн-банкинг, платежные системы, финансовые базы данных, финансовая коммуникация, кибербезопасность, управление ключами.

Leyla Nadir Ibadova
E-mail: leilaibadova594@gmail.com,

Parviz Akhmad Gurbanov
Academy of Public Administration under the President of the Republic of Azerbaijan
associate professor of the Department of “Information Technologies in Public Administration”
doctor of Philosophy in Economics
E-mail: parviz.gurban@gmail.com

Applications of symmetric encryption in finance

Summary

The main purpose of the research - is to determine the security advantages of symmetric encryption, to assess the effectiveness of symmetric encryption in the financial sector, its benefits for financial institutions and users, and to examine the main aspects of its application in financial communications.

Key management methods, security analysis, standards and legal compliance methods were applied **as research methodology** - These methods propose various approaches to increase the effectiveness of symmetric encryption in the financial sector and further develop it.

The significance of the research - is multifaceted. The study will stimulate the development of stronger encryption methods. The information obtained as a result of the study can help banks and other financial institutions use more modern and reliable methods to protect customer information. This, in turn, will have a positive impact on the overall efficiency of the economy.

The results of the research - Symmetric encryption plays an important role in protecting the security and confidentiality of information in financial services. The issues of secure management and sharing of keys still remain a key issue. This study emphasizes the need to develop improved methods and protocols for more secure and efficient application of encryption algorithms in financial systems.

The originality and scientific novelty of the research - It stimulates the development and evaluation of new methods, taking into account the advantages and weaknesses of existing encryption algorithms. Key management and storage issues are one of the important factors affecting the effectiveness of encryption. The development of new methods in this area can be one of the main scientific innovations of the study.

Key words: Symmetric encryption, finance, online banking, payment systems, financial databases, financial communication, cybersecurity, key management.