DOI: https://doi.org/10.36719/2789-6919/56/211-215

Orxan Cəbrayılzadə
Azərbaycan Dövlət Neft və Sənaye Universiteti
magistrant
https://orcid.org/0009-0000-3498-2071
cabrayilzadaorkhan@gmail.com

İnformasiyanın qorunmasında kriptoqrafik üsulların effektivliyinin müqayisəli təhlili və adaptiv tətbiq modeli

Xülasə

Rəqəmsal texnologiyaların sürətli inkişafı və kibertəhdidlərin artması müasir informasiya sistemlərində məlumat təhlükəsizliyinin təmin edilməsini mühüm məsələlərdən birinə çevirmişdir. İnformasiya sistemlərində məlumatın məxfiliyinin, bütövlüyünün və autentikliyinin qorunması üçün kriptoqrafik mexanizmlər geniş şəkildə tətbiq olunur. Müxtəlif kriptoqrafik alqoritmlər fərqli təhlükəsizlik səviyyəsi və performans göstəricilərinə malik olduğuna görə onların seçilməsi zamanı yalnız nəzəri təhlükəsizlik xüsusiyyətləri deyil, həm də praktik tətbiq effektivliyi nəzərə alınmalıdır. Bu məqalədə geniş istifadə olunan simmetrik və asimmetrik kriptoqrafik alqoritmlər — AES-256, RSA-2048 və ECC-256 — təhlükəsizlik səviyyəsi, icra müddəti və resurs sərfiyyatı kimi əsas parametrlər baxımından müqayisəli şəkildə təhlil edilmişdir. Aparılan təhlil nəticəsində kriptoqrafik alqoritmlərin təhlükəsizlik və performans göstəricilərinin inteqrasiyalı qiymətləndirilməsi üçün Kriptoqrafik Effektivlik İndeksi (KEI) adlı model təklif edilmişdir. Bundan əlavə, sistemin risk səviyyəsini, hesablama resurslarını və performans tələblərini nəzərə alan adaptiv seçim mexanizmi formalaşdırılmışdır.

Tədqiqatın nəticələri göstərir ki, bütün informasiya sistemləri üçün vahid universal kriptoqrafik həll mövcud deyil. Kriptoqrafik alqoritmlərin seçilməsi konkret tətbiq mühitinin xüsusiyyətləri, təhlükəsizlik tələbləri və sistem resursları nəzərə alınmaqla həyata keçirilməlidir.

Açar sözlər: *kriptoqrafiya, informasiya təhlükəsizliyi, AES, RSA, ECC, performans analizi, adaptiv model*

Orkhan Jabrayilzadeh
Azerbaijan State Oil and Industry University
Master's student
https://orcid.org/0009-0000-3498-2071
cabrayilzadaorkhan@gmail.com

Comparative Analysis of the Effectiveness of Cryptographic Methods in İnformation Protection and Adaptive Application Model

Abstract

The rapid development of digital technologies and the increasing number of cyber threats have made information security one of the most critical challenges in modern information systems. Cryptographic mechanisms are widely applied to ensure the confidentiality, integrity, and authenticity of data. This study presents a comparative analysis of AES-256, RSA-2048, and ECC-256 algorithms evaluated by security level, execution time, and resource consumption. A formal evaluation model called the Cryptographic Efficiency Index (KEI) is proposed, together with an adaptive selection mechanism that considers system risk level, available computational resources, and performance requirements. Results indicate that no universal cryptographic solution exists for all systems; selection must be guided by the specific application environment and security requirements.

Keywords: *cryptography, information security, AES, RSA, ECC, performance analysis, adaptive model*

Giriş

Müasir informasiya cəmiyyətində rəqəmsal məlumatların həcmi və informasiya sistemlərinin mürəkkəbliyi sürətlə artmaqdadır. Elektron hökumət sistemləri, bank infrastrukturları, bulud texnologiyaları və müxtəlif şəbəkə əsaslı xidmətlər müasir rəqəmsal mühitin əsas komponentlərini təşkil edir. Bu sistemlərdə saxlanılan məlumatların məxfiliyinin, bütövlüyünün və autentikliyinin qorunması informasiya təhlükəsizliyinin əsas prioritetlərindən biri hesab olunur. Məlumatların icazəsiz əldə olunmasının, dəyişdirilməsinin və ya məhv edilməsinin qarşısını almaq üçün kriptoqrafik mexanizmlər geniş şəkildə tətbiq edilir (Stallings, 2017; National Institute of Standards and Technology, 2013).

Kriptoqrafiya informasiya təhlükəsizliyinin təmin edilməsində istifadə olunan riyazi və alqoritmik metodların məcmusudur və məlumatların təhlükəsiz ötürülməsi və saxlanılması üçün əsas texnoloji vasitələrdən biri hesab olunur. Müasir kriptoqrafik sistemlər əsasən iki əsas yanaşmaya əsaslanır: simmetrik və asimmetrik şifrələmə mexanizmləri. Simmetrik kriptoqrafiya məlumatların sürətli şifrələnməsi üçün istifadə olunur, asimmetrik kriptoqrafiya isə açar mübadiləsi və rəqəmsal imza kimi təhlükəsizlik xidmətlərinin təmin edilməsində mühüm rol oynayır (Katz və Lindell, 2015). Bu məqalənin məqsədi geniş istifadə olunan AES-256, RSA-2048 və ECC-256 kriptoqrafik alqoritmlərinin təhlükəsizlik və performans göstəriciləri baxımından müqayisəli təhlilini aparmaq və onların tətbiqi üçün adaptiv seçim modelini təklif etməkdir. Bu məqsədlə kriptoqrafik alqoritmlərin effektivliyini qiymətləndirmək üçün Kriptoqrafik Effektivlik İndeksi (KEI) adlı model təqdim olunur və müxtəlif sistem mühitləri üçün adaptiv kriptoqrafik seçim mexanizmi əsaslandırılır.

Tədqiqat

1. Kriptoqrafik alqoritmlərin təhlili. Simmetrik kriptoqrafiya eyni açardan həm şifrələmə, həm də deşifrələmə proseslərində istifadə olunması prinsipi əsasında qurulur. Bu yanaşma yüksək hesablama sürəti və nisbətən aşağı resurs sərfiyyatı ilə xarakterizə olunur. Bu səbəbdən simmetrik alqoritmlər böyük həcmli məlumatların şifrələnməsi üçün geniş istifadə olunur. Müasir kriptoqrafik sistemlərdə ən geniş yayılmış simmetrik alqoritmlərdən biri Advanced Encryption Standard (AES) hesab olunur. AES müxtəlif açar ölçüləri ilə istifadə oluna bilər və xüsusilə AES-256 variantı yüksək təhlükəsizlik səviyyəsinə görə geniş tətbiq olunur (Stallings, 2017; Menezes və b., 2018; National Institute of Standards and Technology, 2024).

Asimmetrik kriptoqrafiya isə açıq və gizli açar cütlüyü prinsipinə əsaslanır. Bu mexanizmlər əsasən açar mübadiləsi, rəqəmsal imza və autentifikasiya kimi təhlükəsizlik xidmətlərinin təmin edilməsində istifadə olunur. Asimmetrik kriptoqrafiyanın ən geniş yayılmış alqoritmlərindən biri RSA alqoritmidir. RSA böyük sadə ədədlərin faktorizasiyasının riyazi çətinliyinə əsaslanır və uzun illər ərzində informasiya təhlükəsizliyi sistemlərində əsas mexanizmlərdən biri kimi istifadə olunmuşdur (Rivest və b., 1978; Diffie və Hellman, 1976). Son illərdə isə elliptik əyrilər kriptoqrafiyasına əsaslanan alqoritmlər daha geniş tətbiq olunmağa başlamışdır. Elliptic Curve Cryptography (ECC) daha kiçik açar ölçüsü ilə eyni təhlükəsizlik səviyyəsini təmin etməsi səbəbindən xüsusilə mobil qurğular və resurs məhdud sistemlər üçün daha səmərəli hesab olunur (Hankerson və b., 2004; National Institute of Standards and Technology, 2001).

Bu parametrlər arasında təhlükəsizlik səviyyəsi, açar ölçüsü, icra müddəti, hesablama mürəkkəbliyi, resurs sərfiyyatı və tətbiq mühitinə uyğunluq əsas göstəricilər kimi çıxış edir.

Bu parametrlər əsasında AES-256, RSA-2048 və ECC-256 alqoritmlərinin müqayisəli xüsusiyyətləri Cədvəl 1-də təqdim edilmişdir.

Cədvəl 1.

Kriptoqrafik alqoritmlərin müqayisəli xüsusiyyətləri

№	Alqoritm	Təhlükəsizlik səviyyəsi	İcra sürəti	Resurs tələbi	Tətbiq sahəsi
1	AES-256	Çox yüksək	Yüksək	Orta	Məlumat şifrələnməsi
2	RSA-2048	Yüksək	Aşağı	Yüksək	Açar mübadiləsi, rəqəmsal imza
3	ECC-256	Çox yüksək	Orta	Aşağı	Mobil və IoT sistemləri

Cədvəl 1 göstərir ki, AES yüksək icra sürətinə görə böyük həcmli məlumatların şifrələnməsi üçün daha əlverişlidir. RSA isə açar mübadiləsi və rəqəmsal imza mexanizmlərində geniş istifadə olunsa da, yüksək hesablama mürəkkəbliyi səbəbindən performans baxımından daha ağır hesab olunur. ECC isə daha kiçik açar ölçüsü ilə yüksək təhlükəsizlik səviyyəsi təmin etdiyi üçün mobil və IoT sistemləri kimi resurs məhdud mühitlərdə daha səmərəli seçim hesab olunur (Paar və Pelzl, 2010; Boneh və Shoup, 2020; ISO/IEC, 2022).

Lakin bu müqayisə əsasən keyfiyyət göstəricilərinə əsaslanır və alqoritmlərin ümumi effektivliyini vahid ölçü ilə qiymətləndirməyə imkan vermir. Bu səbəbdən kriptoqrafik mexanizmlərin təhlükəsizlik və performans parametrlərini inteqrasiyalı şəkildə qiymətləndirən formal modelin tətbiqi zəruri hesab olunur.

2. Tədqiqat metodologiyası. Analiz üçün üç alqoritm seçilmişdir: AES-256 (simmetrik şifrələmə alqoritmi), RSA-2048 (asimmetrik açıq açarlı alqoritm) və ECC-256 (elliptik əyrilər kriptoqrafiyası). Qiymətləndirmə prosesi kriptoqrafik alqoritmlərin təhlükəsizlik səviyyəsinin müəyyən edilməsini, icra müddətinin və hesablama mürəkkəbliyinin təhlilini, resurs sərfiyyatının (CPU və yaddaş istifadəsi) qiymətləndirilməsini və parametrlərin normallaşdırılmış şkala üzrə qiymətləndirilməsini əhatə edir.

3. Kriptoqrafik effektivlik indeksi (KEI). Cədvəl 1-də təqdim olunan göstəricilərin inteqrasiyalı şəkildə qiymətləndirilməsi məqsədilə Kriptoqrafik Effektivlik İndeksi (KEI) təklif olunur. Bu indeks kriptoqrafik alqoritmlərin təhlükəsizlik səviyyəsi və performans göstəriciləri arasında mövcud olan balansı formal şəkildə ifadə etməyə imkan verir (Bernstein və Lange, 2017; Diffie və Hellman, 1976). KEI modeli müxtəlif kriptoqrafik mexanizmlərin praktik tətbiq effektivliyini müqayisəli şəkildə qiymətləndirmək üçün istifadə olunur.

Kriptoqrafik effektivlik indeksi aşağıdakı kimi müəyyən edilir:

$$KEI = \frac{S}{T+R} \quad (1)$$

(1) düsturunda:

- S – normallaşdırılmış təhlükəsizlik səviyyəsi;
- T – nisbi icra müddəti;
- R – nisbi resurs sərfiyyatı.

Modelin əsas məntiqi ondan ibarətdir ki, təhlükəsizlik səviyyəsinin artması kriptoqrafik alqoritmin ümumi effektivliyini yüksəldir. Eyni zamanda icra müddətinin və resurs sərfiyyatının artması sistem performansına mənfi təsir göstərdiyinə görə effektivlik göstəricisinin azalmasına səbəb olur. Beləliklə, bu model təhlükəsizlik və performans parametrlərinin qarşılıqlı təsirini vahid analitik göstəricidə ifadə etməyə imkan verir.

Cədvəl 2.
KEI göstəriciləri üzrə müqayisəli nəticələr

№	Alqoritm	S	T	R	KEI
1	AES-256	5	2	3	1.0
2	RSA-2048	4	5	5	0.4
3	ECC-256	5	3	2	1.0

Parametrlər müxtəlif kriptoqrafiya mənbələrində təqdim olunan performans xüsusiyyətlərinə əsasən normallaşdırılmış qiymətlərlə müəyyən edilmişdir.

Cədvəl 2-də təqdim olunan nəticələr göstərir ki, RSA alqoritmi təhlükəsizlik baxımından yetərli səviyyəyə malik olsa da, yüksək icra müddəti və resurs sərfiyyatı səbəbindən onun effektivlik indeksi digər alqoritmlərlə müqayisədə daha aşağıdır. AES və ECC alqoritmləri isə müxtəlif tətbiq mühitlərində daha balanslı təhlükəsizlik və performans göstəriciləri təqdim edir.

4. Adaptiv seçim mexanizmi. Model üç əsas parametrə əsaslanır: RS (sistemin risk səviyyəsi), C (mövcud hesablama resursları) və Tq (real vaxt tələbi).

Bu parametrlərin kombinasiyası əsasında kriptoqrafik alqoritmlərin seçilməsi üçün aşağıdakı qərar prinsipləri müəyyən edilmişdir:

1. Risk səviyyəsi yüksək və sistem resursları məhdud olduqda ECC əsaslı mexanizmlər daha uyğun hesab olunur;
2. Risk səviyyəsi yüksək və sistem resursları geniş olduqda AES və RSA alqoritmlərinin hibrid tətbiqi daha effektiv nəticə verir;
3. Risk səviyyəsi orta və real vaxt tələbi yüksək olduqda AES alqoritmi əsas şifrələmə mexanizmi kimi istifadə oluna bilər.

5. Adaptiv tətbiq çərçivəsi. Təklif olunan adaptiv tətbiq çərçivəsi kriptoqrafik alqoritmlərin seçilməsi prosesini sistemli şəkildə həyata keçirməyə imkan verir və üç əsas mərhələdən ibarətdir:

1. Sistemin təhlükəsizlik və texniki parametrlərinin qiymətləndirilməsi;
2. Seçilmiş alqoritmlər üçün KEI indeksinin hesablanması;
3. Tətbiq mühitinə uyğun optimal kriptoqrafik mexanizmin seçilməsi.

Nəticə

Aparılan tədqiqat nəticəsində aşağıdakı əsas nəticələr əldə edilmişdir:

1. Kriptoqrafik alqoritmlərin effektivliyi yalnız təhlükəsizlik səviyyəsi ilə müəyyən edilmir. Praktik informasiya sistemlərində alqoritmin seçilməsi zamanı icra müddəti, hesablama mürəkkəbliyi və sistem resurslarının istifadəsi kimi performans göstəriciləri də nəzərə alınmalıdır.
2. Məqalədə AES-256, RSA-2048 və ECC-256 alqoritmləri təhlükəsizlik və performans parametrləri baxımından müqayisəli şəkildə təhlil edilmişdir və bu alqoritmlərin müxtəlif tətbiq mühitlərində fərqli üstünlüklərə malik olduğu göstərilmişdir.
3. Aparılan təhlil əsasında kriptoqrafik alqoritmlərin təhlükəsizlik və performans göstəricilərinin inteqrasiyalı qiymətləndirilməsi üçün Kriptoqrafik Effektivlik İndeksi (KEI) modeli təklif edilmişdir.
4. Bundan əlavə, sistemin risk səviyyəsini, hesablama resurslarını və performans tələblərini nəzərə alan adaptiv seçim mexanizmi və onun tətbiqi üçün sadələşdirilmiş tətbiq çərçivəsi təqdim edilmişdir.

Beləliklə, müasir informasiya sistemlərində kriptoqrafik mexanizmlərin seçilməsi statik yanaşmaya deyil, sistem mühitinin xüsusiyyətlərini nəzərə alan adaptiv prinsiplərə əsaslanmalıdır.

Ədəbiyyat

1. Bernstein, D. və Lange, T. (2017). *Post-Quantum Cryptography*. Nature.
2. Boneh, D. və Shoup, V. (2020). *A Graduate Course in Applied Cryptography*. Stanford University.
3. Diffie, W., Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.
4. Hankerson, D., Menezes, A. və Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer.
5. ISO/IEC. (2022). *ISO/IEC 27001: Information Security Management Systems — Requirements*. International Organization for Standardization.
6. Katz, J. və Lindell, Y. (2015). *Introduction to Modern Cryptography*. CRC Press.
7. Menezes, A., van Oorschot, P. və Vanstone, S. (2018). *Handbook of Applied Cryptography*. CRC Press.
8. National Institute of Standards and Technology. (2001). *FIPS 197: Advanced Encryption Standard (AES)*. NIST.
9. National Institute of Standards and Technology. (2013). *FIPS 186-4: Digital Signature Standard (DSS).* NIST.
10. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework (CSF) 2.0.* NIST.

11. Paar, C. və Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
12. Rivest, R., Shamir, A. və Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126.
13. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

Daxil oldu: 26.11.2025
Qəbul edildi: 03.03.2026