MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere
Șefă departament:
Tîrșu Valentina, conf. univ., dr.

_____

„____” _____ 2024

Analiza și implementarea mecanismelor de securitate cibernetică în dezvoltarea aplicațiilor Java

Teză de master

Student: **Petrușca Dorin**
gr. SISRC-221M

Conducător: **Cerbu Olga**
conf. univ., dr.

Chișinău, 2024

ADNOTARE

Autorul: Petrușca Dorin, gr. SISRC-221M

Tema: Analiza și implementarea mecanismelor de securitate cibernetică în dezvoltarea aplicațiilor Java

Structura lucrării: constă din pagini de titlu, aviz, rezumat, introducere, 3 capitole, concluzii, bibliografie și anexe.

Cuvinte cheie: criptografie, serializare, deserializare, AES, Java.

Problematica studiului: Investigarea detaliată a criptografiei și securității cibernetice, cu accent pe analiza conceptelor criptografice, studiul algoritmului AES în limbajul de programare Java, explorarea mecanismelor de serializare și deserializare Java, implementarea practică a criptografiei, și evaluarea securității criptografice în contextul aplicațiilor web.

Scopul lucrării: De a explora și înțelege conceptele esențiale ale criptografiei, precum și de a evalua implementarea și aplicarea acestora în limbajul de programare Java. Prin analiza detaliată a criptării, a algoritmului AES și a mecanismelor de serializare și deserializare, se urmărește dezvoltarea de soluții practice pentru protejarea informației și asigurarea confidențialității datelor în mediul digital.

Obiectivele:

a) Analiza conceptelor criptografice.
b) Studiu detaliat al algoritmului AES.
c) Explorarea mecanismelor de serializare și deserializare Java.
d) Implementarea practică a criptografiei în Java.
e) Evaluarea securității criptografice în aplicații web.

Metode aplicate: În cadrul acestei lucrări, s-au adoptat metode analitice pentru a investiga detaliat aspectele legate de criptografia și securitatea cibernetică. Aceste metode au fost utilizate pentru analiza conceptelor fundamentale ale criptografiei, implementarea algoritmului Advanced Encryption Standard (AES) în limbajul de programare Java, și evaluarea mecanismelor de serializare și deserializare în acest context.

Rezultatele obținute: Această teză de master a realizat cu succes obiectivele propuse prin investigarea amănunțită a criptografiei și securității cibernetice. Rezultatele includ o înțelegere profundă a conceptelor criptografice, cu accent pe avantajele și limitările criptografiei simetrice și asimetrice. Un studiu detaliat al algoritmului AES în limbajul de programare Java a relevat complexitatea și robustețea acestui standard. De asemenea, s-au analizat mecanismele de serializare și deserializare în Java, evidențiind beneficiile, limitările și riscurile asociate. Prin implementarea practică a criptografiei în Java, utilizând Java Cryptography Extension, s-a dezvoltat o aplicație care a testat eficient algoritmul AES și mecanismele de serializare/deserializare.

ANNOTATION

Author: Petruşca Dorin, gr. SISRC-221M

Title: Analysis and implementation of cybersecurity mechanisms in Java application development

Thesis structure: It consists of title pages, approval, abstract, introduction, 3 chapters, conclusions, bibliography, and annexes.

Key words: cryptography, serialization, deserialization, AES, Java.

Research problem: In-depth investigation of cryptography and cybersecurity, with a focus on analyzing cryptographic concepts, studying the AES algorithm in the Java programming language, exploring Java serialization and deserialization mechanisms, practical implementation of cryptography, and evaluating cryptographic security in the context of web applications.

Thesis purpose: To explore and understand the essential concepts of cryptography and evaluate their implementation and application in the Java programming language. Through a detailed analysis of encryption, the AES algorithm, and serialization and deserialization mechanisms, the aim is to develop practical solutions for protecting information and ensuring data confidentiality in the digital environment.

Objectives:

a) Analyze cryptographic concepts.

b) Detailed study of the AES algorithm.

c) Explore Java serialization and deserialization mechanisms.

d) Practical implementation of cryptography in Java.

e) Evaluate cryptographic security in web applications.

Applied methods: In this thesis, analytical methods were adopted to thoroughly investigate aspects related to cryptography and cybersecurity. These methods were used to analyze fundamental cryptographic concepts, implement the Advanced Encryption Standard (AES) algorithm in the Java programming language, and evaluate serialization and deserialization mechanisms in this context.

The obtained results: This master's thesis successfully achieved its objectives through a detailed investigation of cryptography and cybersecurity. The results include a deep understanding of cryptographic concepts, with a focus on the advantages and limitations of symmetric and asymmetric cryptography. A detailed study of the AES algorithm in the Java programming language revealed the complexity and robustness of this standard. Additionally, Java serialization and deserialization mechanisms were analyzed, highlighting their benefits, limitations, and associated risks. Through the practical implementation of cryptography in Java, using Java Cryptography Extension, an application was developed that effectively tested the AES algorithm and serialization/deserialization mechanisms.

CUPRINS

INTRODUCERE

Cum să se transmită informația corectă destinatarului potrivit, în secret față de ceilalți?

Fiecare dintre cititori, în momente diferite și cu scopuri diferite, au încercat probabil să rezolve această problemă practică. Gândind la această problemă, este ușor de concluzionat că există trei posibilități:

a) Crearea unui canal de comunicare complet fiabil și inaccesibil între abonați.

b) Să se utilizeze un canal de comunicare accesibil publicului, dar să se ascundă faptul transmiterii informațiilor.

c) Să se utilizeze un canal de comunicare accesibil publicului, dar să se transmită informația dorită într-o formă transformată astfel încât numai destinatarul să o poată reconstrui.

Nu există absolut nicio modalitate de a înțelege dezvoltarea societății umane în afara dorinței sale arzătoare de a avea secrete. Politicieni și militari, preoți și negustori, scriitori și oameni de știință, șarlatani și escroci au dezvoltat știința secretelor timp de mii de ani, aducându-și creația la perfecțiune, slujind secretele, satisfăcându-și nevoile în ele. Fără secrete nu poate exista nu doar un stat, ci chiar și o mică comunitate de oameni - fără ele nu se poate câștiga o bătălie sau vinde bunuri în mod profitabil, nu se pot învinge adversarii politici într-o luptă aprigă pentru putere, nu se poate menține superioritatea în domeniul tehnologiei. Secretele stau la baza științei, tehnologiei și politicii oricărei formațiuni umane, fiind cimentul statalității.

Istoria deține atât de multe secrete, încât este uimitor cât de mult au nevoie oamenii de ele. Serviciile de securitate încearcă să le împartă pe mai multe niveluri: de la pentru uz oficial la strict secret și strict confidențial. Fizicianul american Richard Feynman glumea spunând că, atunci când lucra la bomba atomică, pe lângă documentele pe care scria "ingest after reading", adică mâncați literalmente după ce citiți, a dat uneori peste hârtii cu o ștampilă pe care scria să le distrugă înainte de a le citi. Oricât de științifică ar fi teoria din spatele unei astfel de clasificări, aceasta se reduce la o discriminare obișnuită împotriva unor grupuri de oameni, încălcându-le drepturile naturale. Dacă delapidările financiare pot fi împărțite legal în mici și mari, este absurd să clasificăm gradul de secretizare. Raportul lui Hrușciov privind cultul personalității lui Stalin de la cel de-al 20-lea Congres al partidului părea secret doar pentru aparatul de partid, dar nu și pentru majoritatea oamenilor obișnuiți, care cunoșteau foarte bine situația din societate.

Secretul pentru fiecare individ în parte fie că există, fie că nu există. În plus, nu numai că nu este o infracțiune să dezvălui un secret în mod analitic, dar este un triumf al rațiunii umane și ar trebui să fie binevenit, dacă este făcut în mod deschis și cu cele mai bune intenții. Francezii spun: "Este moștenirea zeilor să creeze mistere, iar al regilor să le rezolve". Într-adevăr, arătați-le experților doar o singură piesă dintr-un dispozitiv complex și ei îi vor reconstitui forma, scopul și caracteristicile complete.

Guvernele din întreaga lume încearcă să priveze oamenii de intimitate: scrisorile sunt citite, telefoanele sunt ascultate, bagajele și portbagajele sunt percheziționate, oamenii sunt supravegheați. În același timp, din ce în ce mai multe dintre comunicațiile noastre private trec prin canale electronice. Mai

întâi au fost telefoanele, apoi au fost faxurile, iar în cele din urmă există e-mailul. Mesajele de e-mail sunt deosebit de ușor de interceptat sau scanat prin a găsi cuvinte-cheie, lucru pe care îl fac pe scară largă agențiile guvernamentale, hackerii și curioșii deopotrivă. Persoane care consideră că confidențialitatea conținutului scrisorilor, telegramelor și conversațiilor lor telefonice sunt protejate de Constituție, ar trebui să realizeze că aceasta acordă doar dreptul la o astfel de protecție, dar să ne apere direct nu o poate face pentru fiecare în parte.

Scopul acestei lucrări este de a explora și înțelege conceptele esențiale ale criptografiei, precum și de a evalua implementarea și aplicarea acestora în limbajul de programare Java. Prin analiza detaliată a criptării, a algoritmului AES și a mecanismelor de serializare și deserializare, se urmărește dezvoltarea de soluții practice pentru protejarea informației și asigurarea confidențialității datelor în mediul digital.

Pentru a atinge acest scop, această lucrare își propune următoarele **obiective** specifice:

a) Analiza conceptelor criptografice: investigarea detaliată a conceptelor de criptare simetrică și asimetrică, precum și a obiectivelor criptografice pentru a obține o înțelegere cuprinzătoare a fundamentelor securității cibernetice.

b) Studiu detaliat al algoritmului AES: examinarea în profunzime a structurii și funcționării algoritmului Advanced Encryption Standard (AES) pentru a înțelege implementarea sa în limbajul de programare Java.

c) Explorarea mecanismelor de serializare și deserializare Java: investigarea mecanismelor de serializare și deserializare în limbajul de programare Java, evidențiind beneficiile, limitările, riscurile și vulnerabilitățile asociate.

d) Implementarea practică a criptografiei în Java: realizarea unei aplicații practice utilizând Java Cryptography Extension pentru a implementa și testa algoritmul AES și mecanismele de serializare și deserializare.

e) Evaluarea securității criptografice în aplicații web: analizarea modului în care mecanismele de criptare și serializare/deserializare pot fi aplicate în contextul aplicațiilor web, evidențiind exemple de implementare reușită și măsuri de securitate.

BIBLIOGRAFIE

1. RAJANI DEVI T., Importance of Cryptography in Network Security. In: 2013 International Conference on Communication Systems and Network Technologies. New York: IEEE, 2013, p. 1, ISBN 978-1-4673-5088-6, DOI: 10.1109/CSNT.2013.102, [citat 15.10.2023], Disponibil: https://ieeexplore.ieee.org/document/6524439
2. SCHNEIER B., Why cryptography is harder than it looks. In: Secure Internet Programming. Berlin: Springer, 1999, p. 3, ISBN 978-3-540-66130-4, [citat 18.10.2023], Disponibil http://www.firstnetsecurity.com/library/counterpane/whycrypto.pdf
3. SALAMA D., ELMINAAM A., MOHAMED H., KADER A., HADHOUD M., Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security, vol. 8, no. 12, 2008, p. 280-286, ISSN 1738-7906, [citat 19.10.2023], Disponibil: https://www.academia.edu/download/67227755/20081240.pdf
4. KETU FILE, Symmetric vs Asymmetric Encryption. A division of Midwest Research Corporation, 2004, [citat 21.10.2023], Disponibil: https://core.ac.uk/download/pdf/228547549.pdf
5. Difference between AES and DES ciphers, GeeksforGeeks, 2019, [citat 17.12.2023], Disponibil: https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/
6. Java Cryptography Architecture (JCA) Reference Guide, Oracle, 2006, [citat 15.12.2023], Disponibil: https://docs.oracle.com/javase//1.5.0/docs/guide/security/jce/JCERefGuide.html
7. BEAVER K., Achieving Sarbanes-Oxley compliance for Web applications through security testing. SPI Dynamics, 2003.
8. HULME G., New software may improve application security. InformationWeek, 2001.
9. WAGNER D., FOSTER J., BREWER E., AIKEN A., A first step towards automated detection of buffer overrun vulnerabilities. In: Proceedings of Network and Distributed Systems Security Symposium. San Diego: Internet Society, 2000, p. 3-17, ISBN 1-891562-06-5, [citat 25.11.2023], Disponibil: https://www.cs.umd.edu/class/spring2021/cmsc614/papers/automated-buffer.pdf
10. ANLEY C., Advanced SQL injection in SQL Server applications. Next Generation Security Software, 2002, [citat 27.11.2023], Disponibil: https://www.academia.edu/download/53070642/advanced_sql_injection.pdf
11. SURF M., SHULMAN A., How safe is it out there? Imperva, 2004.
12. WALL L., CHRISTIANSEN T., SCHWARTZ R., Programming Perl. Sebastopol: O'Reilly and Associates, 1996, p. 646, ISBN 978-1-56592-149-8.
13. ȚURCANU D., SPINU N., POPOVICI S., ȚURCANU T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.

14. PECA L., ȚURCANU D. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.
15. BULAI R., CIORBĂ D, ȚURCANU D. Education in Cybersecurity, Central and Eastern European e|Dem and e|Gov Days 2019 Budapest, Hungary, 2-3 mai 2019.
16. HOWARD M., LEBLANC D., Writing Secure Code. Redmond: Microsoft Press, 2001, p. 800, ISBN 978-0-7356-1588-8.
17. KLEIN A., Hacking Web applications using cookie poisoning, CGISecurity, 2002.
18. LIVSHITS V.B., LAM M.S., Finding Security Vulnerabilities in Java Applications with Static Analysis. In: 14th USENIX Security Symposium. Berkeley: USENIX Association, 2005, p. 271-286, ISBN 1-931971-36-5, [citat 15.12.2023], Disponibil: https://www.usenix.org/legacy/publications/library/proceedings/sec05/tech/full_papers/livshits/livshits.pdf
19. GUPTA N., KAPOOR V., Hybrid cryptographic technique to secure data in web application. Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 1, 2020, p. 125-135, DOI: 10.1080/09720529.2020.1721872, [citat 05.12.2023] Disponibil: https://www.tandfonline.com/doi/abs/10.1080/09720529.2020.1721872
20. BUEGE B., LAYMAN R., TAYLOR A., Hacking Exposed: J2EE and Java: Developing Secure Applications with Java Technology. Emeryville: McGraw-Hill/Osborne, 2002, p. 512, ISBN 978-0-07-222710-9.
21. Serializare în Java - Ghid pentru serializarea Java cu exemple, CodeGym, 2019, [citat 16.12.2023], Disponibil: https://codegym.cc/groups/posts/217-java-serialization-formats
22. Spring Boot, Spring, 2021, [citat 19.12.2023], Disponibil: https://spring.io/projects/spring-boot/
23. Spring Boot Maven Plugin, [citat 19.12.2023], Disponibil: https://docs.spring.io/spring-boot/docs/2.2.2.RELEASE/maven-plugin/
24. Running a Spring Boot App with Maven vs an Executable War/Jar, [citat 19.12.2023], Disponibil: https://www.baeldung.com/spring-boot-run-maven-vs-executable-jar
25. Baza de date PostgreSQL, [citat 19.12.2023], Disponibil: https://www.postgresql.org/download/
26. Aplicația Postman, [citat 19.12.2023], Disponibil: https://www.postman.com/downloads/