Dezvoltarea unei aplicatii pentru criptarea datelor utilizand arhitectura JCA (Java Criptography Architecture)

Introducere – tema lucrarii, importanta ei in contextual actual, o enumerare a tehnologiilor utilizate pentru dezvoltarea aplicatiei

Capitolul 1 – Prezentarea generala a tehnologiilor utilizate – Java (JCA, swing)

Capitolul 2 – Arhitectura aplicatiei – baze de date, clase, modul utilizator, admin – clase utilizate. Secvente de cod.

Capitolul 3 – Functionalitatea aplicatiei (un fel de ghid de utilizare)/

Capitolul 4 - descrierea algoritmilor criptografici

Concluzii – tema lucrarii, directii viitoare de dezvoltare – criptare video/audio ca directie

Introducere – tema lucrarii, importanta ei in contextual actual, o enumerare a tehnologiilor utilizate pentru dezvoltarea aplicatiei

Introducere

Criptografia este arta si stiinta prepararii codate sau protejate a comunicatiilor care trebuie sa fie inteligibile doar pentru persoana care are o cheie in posesie. Criptografia (greaca, *kryptos*, "ascuns", *graphos* "a scrie" ) se refera la procesul de a comunica in sau de a descifra scrieri ascunse (coduri sau cifruri), dar si la folosirea de coduri pentru a converti date computerizate in asa fel incat numai un recipient anume sa le poata citi folosind o cheie (criptare). Criptografii definesc ca text clar sau text simplu o comunicatie originala. Odata ce comunicatia originala a fost criptata, rezultatul este cunoscut ca text cifrat sau criptograma. Procesul de cifrare implica de obicei un algoritm si o cheie. Un algoritm de criptare este o metoda particulara de amestecare – un program de calculator sau un set de instructiuni scrise. Cheia specifica procesul de amestecare. Comunicatia originala poate fi un mesaj scris sau difuzat sau un set de date digitale.

In sensul mai larg, criptografia include folosirea de mesaje ascunse, cifruri si coduri. Mesajele ascunse, asemeni celor ascunse in text la vedere sau celor scrise cu cerneala invizibila , depinde de succesul lor de a nu fi suspectate. Odata ce sunt descoperite, sunt in mod frecvent usor de descifrat. Codurile, in care cuvintele, numerele sau simbolurile reprezinta cuvinte si fraze, sunt de obicei imposibil de citit fara cheia dictionarului. Criptografia include, de asemenea, folosirea criptarii computerizate pentru protejarea transmisiilor de date si mesaje.

Criptografia – proces general:

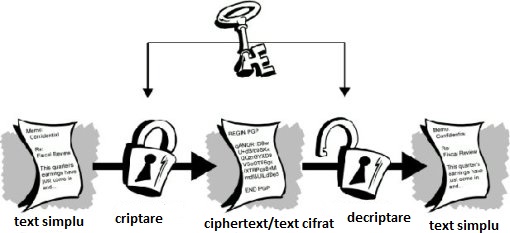


Fig.1-Criptografia – descriere proces

* 1. Istoric

Inainte de epoca moderna, criptografia se ocupa doar cu asigurarea confidentialitatii mesajelor si inversul acestui proces pentru a face mesajul imposibil de inteles pentru cei care intercepteaza mesajul si nu detin cheia necesara decriptarii mesajului. Cele mai vechi forme de scriere secretizata necesitau doar putin mai mult decat unelte de scris si hartie deoarece majoritatea oamenilor nu stiau sa citeasca. Cu timpul, complexitatea criptografiei a crescut deoarece a crescut si alfabetizarea. Principalele tipuri clasice de cifruri sunt [cifrurile cu transpoziție](https://ro.wikipedia.org/w/index.php?title=Cifru_cu_transpozi%C8%9Bie&action=edit&redlink=1" \o "Cifru cu transpoziție — pagină inexistentă), care modifică ordinea literelor dintr-un mesaj (de exemplu „ajutor” devine „ojartu” într-o schemă trivială de rearanjare), și [cifrurile cu substituție](https://ro.wikipedia.org/w/index.php?title=Cifru_cu_substitu%C8%9Bie&action=edit&redlink=1" \o "Cifru cu substituție — pagină inexistentă), care înlocuiesc sistematic litere sau grupuri de litere cu alte litere și grupuri de litere (de exemplu, „conexiune” devine „dpofyjvof” înlocuind fiecare literă cu următoarea din alfabet). Versiuni simple ale celor două tipuri de cifruri ofereau un grad mic de confidențialitate în cazul oponenților instruiți. Unul din primele cifruri cu substituție a fost [Cifrul lui Cezar](https://ro.wikipedia.org/wiki/Cifrul_lui_Cezar" \o "Cifrul lui Cezar), în care fiecare literă din textul clar era înlocuită cu o literă aflată la un număr fix de poziții distanță de ea în alfabet. Cifrul a fost denumit astfel după [Iulius Cezar](https://ro.wikipedia.org/wiki/Iulius_Cezar" \o "Iulius Cezar) despre care se spune că l-a folosit, cu o deplasare de 3, în comunicația cu generalii săi în timpul campaniilor militare. In ultimele 2 decenii, domeniul s-a extins dincolo de problemele de confidentialitate si include, printre altele, si tehnici de verificare a integritatii mesajului, autentificarea trimitatorului si a receptorului, semnatura electronica, calcule securizate.

* 1. Importanta criptografiei in contextual actual

Astazi, majoritatea comunicatiilor lasa un fel de urma inregistrata. De exemplu, comunicatiile telefonice, inclusive faxurile si mesajele e-mail, produc o inregistrare a numarului de telefon apelat si timpul la care a fost apelat. Tranzactiile financiare, istoricul medical, alegerea filmelor inchiriate si chiar si alegerea mancarii pot fi urmarite cu chitantele cardului bancar sau inregistrarile asigurarii. De fiecare data cand cineva foloseste un telefon sau un card bancar, compania de telefoane sau institutia financiara tine o inregistrare a numarului apelat sau a sumei tranzactionate, a locatiei si a datei. In viitor, pe masura ce retelele telefonice devin digitale, chiar si conversatiile insesi pot fi inregistrate si stocate. Toate acestea duc catre o mai mare confidentialitate. Abilitatea de a cripta date, comunicatii si alte informatii le da indivizilor puterea de a isi restaura confidentialitatea personala.

Criptografia ofera mai mult decat confidentialitate, totusi. Criptografia protejeaza si sistemele bancare mondiale. Multe banci si alte institutii financiare isi conduc afacerile pe canale deschise, precum internetul. Fara abilitatea de a proteja tranzactiile si comunicatiile bancare, criminalii pot interveni in tranzactii si pot fura bani fara a lasa o urma.

* 1. Tehnologii utilizate

Toate aspectele mentionate mai sus duc la concluzia ca criptografia este o componenta din ce in ce mai necesara desfasurarii activitatilor zilnice individuale, dar si a activitatilor la nivel de system.

Influentata de tendinta de digitalizare si de evolutia tehnologica rapida, imi propun prin aceasta lucrare implementarea unei astfel de aplicatii folosind API-ul oferit de limbajul de programare JAVA prin intermediul librariei JCA (Java Cryptography Architecture ). Aplicatia, inspirata dintr-o nevoie de a ascunde comunicatiile intre trimitator si receptor, se incadreaza in categoria produselor software destinate securizarii unui computer sau a unei retele.

In capitolul 1 este prezentat pe scurt limbajul de programare Java si sunt identificate si analizate solutiile oferite de acesta la provocarile oferite de protejarea si securizarea datelor.

Capitolul 2 face o scurta introducere in lumea dezvoltarii de aplicatii software de securitate si prezinta tehnologiile folosite pentru atingerea obiectivului acestei lucrari. Acesta include libraria Java Criptography Architecture si libraria JFC.

Capitolul 3 descrie in detaliu toate functionalitatile aplicatiei si metodele folosite pentru implementarea acestora.

Capitolul 4 pune accentual pe implementarea algoritmilor criptografici. Sunt prezentati principalii algoritmi de criptare pe tipuri de cheie utilizate si modul in care acestia au fost aplicati in procesul de implementare pentru a se potrivi contextului aplicatiei dezvoltate.

<http://dspace.cusat.ac.in/jspui/bitstream/123456789/2628/1/Cryptography%20and%20Security.pdf>

<https://ro.wikipedia.org/wiki/Criptografie>

https://profs.info.uaic.ro/~adiftene/Licenta/Licenta2013\_Nita%20Iulian-Alexandru.pdf

<https://en.wikipedia.org/wiki/Java_Cryptography_Architecture>

<https://www.webopedia.com/TERM/S/security_software.html>