Protectia si securitatea

documentelor electronice

Wallach Luke & Chanchian Armin Andrei

Cuprins

[Capitolul 1 – Introducere 3](#_Toc134821016)

[1.1 Informatica 3](#_Toc134821017)

[1.2 Securitatea informatiei 3](#_Toc134821018)

[1.3 Criptografia 4](#_Toc134821019)

[Capitolul 2 – Rolul securizarii documentelor in cadrul domeniului IT 5](#_Toc134821020)

[1.1 Definirea conceptului de document electronic 5](#_Toc134821021)

[1.2 Istoria 5](#_Toc134821022)

[1.3 Tipuri 6](#_Toc134821023)

[1.4 Importanta documentelor electronice in societatea moderna 8](#_Toc134821024)

[1.5 Scopul si obiectivele proiectului 9](#_Toc134821025)

[Capitolul 3 – Aprfoundarea tematicii documentelor electronice 10](#_Toc134821026)

[1.1 Riscurile si amenintarile 10](#_Toc134821027)

[Accesul neautorizat 10](#_Toc134821028)

[Virusi si malware 11](#_Toc134821029)

[Atac cibernetic 13](#_Toc134821030)

[Atacurile "man-in-the-middle" 14](#_Toc134821031)

[Expunerea accidentala sau intentionata 14](#_Toc134821032)

[Scaderea perfromantei sistemului informatic 15](#_Toc134821033)

[1.2 Masuri de protectie si securitate pentru documentele electronice 15](#_Toc134821034)

[Autentificare si autorizare 15](#_Toc134821035)

[Criptare 16](#_Toc134821036)

[SSL/TLS 23](#_Toc134821037)

[Firewall si Antivirus 24](#_Toc134821038)

[VPN 25](#_Toc134821039)

[Backup si recuperarea datelor 25](#_Toc134821040)

[Protejarea documentelor cu o parola 28](#_Toc134821041)

[Protectia datelor personale si a confidentialitatii 30](#_Toc134821042)

[Semnatura electronica si digitala 31](#_Toc134821043)

[Politici si proceduri de securitate in cadrul unei companii 32](#_Toc134821044)

[Exemple aplicatii 33](#_Toc134821045)

[Lucru practic 34](#_Toc134821046)

[Capitolul 4 – Concluzii 39](#_Toc134821047)

[Bibliografie 40](#_Toc134821048)

# Introducere

## Informatica

Informatica este studiul calculatoarelor si al informaticii, inclusiv al bazelor teoretice si algoritmice, al hardware-ului si software-ului, precum si al utilizarilor acestora pentru prelucrarea informatiilor.

Disciplina informatica include studiul algoritmilor si al structurilor de date, proiectarea calculatoarelor si a retelelor, modelarea datelor si a proceselor informationale, precum si inteligenta artificiala. Informatica isi extrage unele dintre fundamente din matematica si inginerie si, prin urmare, incorporeaza tehnici din domenii precum teoria statului la coada, probabilitatea si statistica si proiectarea circuitelor electronice.

De asemenea, informatica utilizeaza intensiv testarea ipotezelor si experimentarea in timpul conceptualizarii, proiectarii, masurarii si perfectionarii noilor algoritmi, structuri de informatii si arhitecturi de calculatoare. [1]

Asadar, aceasta disciplina acopera si aspectele de securitate si protectie a informatiilor si datelor.

## Securitatea informatiei

Securitatea informatiilor este un concept care se refera la protejarea informatiilor, a datelor digitale si analogice impotriva accesului neautorizat. Acesta este doar o ramura a unui termen umbrela cuprinzator, necesar in ziua de astazi, si anume managementul riscului informational, implicand astfel prevenirea sau reducerea posibilitatii accesului neautorizat asupra unei baze de date, utilizarea informatiilor in scopuri frauduloase, dezvaluirea, stergerea, coruptia, modificarea sau inregistrarea unor date confidentiale de o persoana sau organizatie straine.

Securitatea informatiilor acopera toate ariile care se refera la mediul cibernetic, deci implicit domeniul IT. Pentru protejarea datelor, acesta utilizeaza instrumente precum autentificarea si permisiunea de a restrictiona accesul utilizatorilor neautorizati asupra informatiilor private.

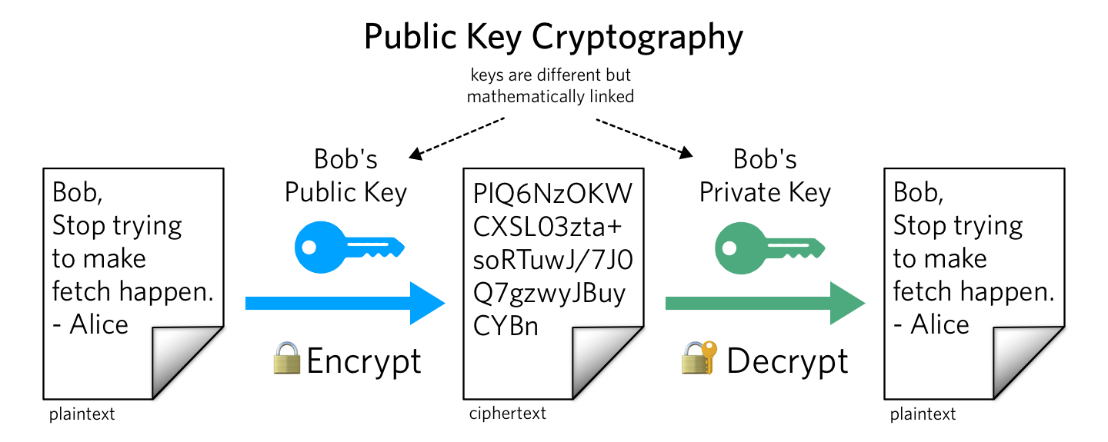
Programele destinate securitatii informatiilor sunt construite in jurul a 3 obiective:

* Confidentialitatea – informatiile nu sunt divulgate persoanelor sau entitatilor neautorizate;
* Integritatea – mentinerea acuratetii si exhaustivitatii datelor. Acest lucru inseamna ca informatiile personale nu pot fi editate si modificate de catre o entitate neautorizata;
* Disponibilitatea – se refera la un anumit tip de date care trebuie sa fie disponibile public fara a afecta identitatea fizica si cibernetica a persoanei sau organizatiei care pune la dispozitie setul de date. [2]

## Criptografia

Criptografia reprezinta o ramura a matematicii care se ocupa cu securizarea informatiei precum si cu autentificarea si restrictionarea accesului intr-un sistem informatic. In realizarea acestora se utilizeaza atat metode matematice (profitand, de exemplu, de dificultatea factorizarii numerelor foarte mari), cat si metode de criptare cuantica. Termenul criptografie este compus din cuvintele de origine greaca κρυπτός (ascuns) si γράφειν grafein (a scrie). [3]

In criptografie, un mesaj original care poate fi citit de catre om, denumit "text simplu", este transformat, prin intermediul unui algoritm sau al unei serii de operatii matematice, in ceva care pentru un observator neinformat ar parea o aberatie; aceasta aberatie se numeste "text cifrat".



\* Criptografia cu cheie publica

\* chei diferite dar legate matematic

\* decriptare

(c) twilio

\* criptare

Sistemele criptografice necesita o anumita metoda pentru ca destinatarul sa poata utiliza mesajul criptat - de obicei, dar nu intotdeauna, prin transformarea textului cifrat in text clar.

Criptografia este utilizata in mod frecvent in securitatea informatiei, inclusiv in protectia datelor personale si a informatiilor financiare.

Criptarea - "a face secret" - este procesul de transformare a textului clar in text cifrat. Criptarea este o parte importanta a criptografiei, dar nu cuprinde intreaga stiinta. Opusul sau este decriptarea.

Un aspect important al procesului de criptare este faptul ca aproape intotdeauna implica atat un algoritm, cat si o cheie. O cheie este doar o alta informatie, aproape intotdeauna un numar, care specifica modul in care algoritmul este aplicat textului clar pentru a-l cripta. Intr-un sistem criptografic sigur, chiar metoda prin care este criptat un mesaj este cunoscuta, ar trebui sa fie dificil sau imposibil de decriptat fara acea cheie. [4]

# Rolul securizarii documentelor in cadrul domeniului IT

## Definirea conceptului de document electronic

Un document electronic este orice continut de informatie memorat in forma electronica (altul decat programele sau fisierele de sistem), destinat a fi utilizat fie ca material tiparit, fie ca atare. In calculator, documentul electronic este reprezentat sub forma unui fisier.

Initial, orice date informatice erau considerate ca fiind ceva intern sistemului de calcul; rezultatul prelucrarii datelor se livra beneficiarului, intotdeauna, pe hartie. Insa retelele de calculatoare au evoluat in asa fel incat, in cele mai multe cazuri, oferirea documentelor electronice devine mai convenabila decat cea a documentelor tiparite. Progresele tehnologiilor de afisare digitala fac ca, in cele mai multe cazuri, sa fie mai comoda vizualizarea documentele pe ecran, in loc de a le tipari (economisind astfel hartie si spatiul necesar pentru stocarea exemplarelor tiparite).[5]

Documentele electronice pot fi create in diferite formate, cum ar fi documente text, prezentari, fisiere multimedia, etc. In contrast cu documentele traditionale pe suport fizic, acestea pot fi accesate si distribuite rapid si la nivel global, fara a fi nevoie de transport fizic.

## Istoria

Inca din anii 1950, au fost dezvoltate sisteme informatice care puteau stoca si procesa cantitati mari de date, inclusiv documente text.

Una dintre primele forme de documente electronice a fost formatul de fisier ASCII, care a fost dezvoltat in in anii '60. ASCII (American Standard Code for Information Interchange) este modalitate standardizata de codificare a caracterelor textului, care permitea citirea si manipularea usoara a acestora de catre programele de calculator. Acest format este utilizat pe scara larga si in prezent pentru documente text simple.

In anii '70, dezvoltarea calculatorului personal a dus la crearea unor formate de documente mai sofisticate, cum ar fi Rich Text Format (RTF) si formatul WordPerfect. Aceste formate au permis utilizatorilor sa creeze documente mai complexe, cu formatare, cum ar fi text bold si italic, dimensiuni diferite ale fonturilor si asa mai departe.

dezvoltarea calculatorului personal a dus la crearea unor formate de documente mai sofisticate, cum ar fi Rich Text Format (RTF), a formatului WordPerfect, si a limbajului PostScript pentru imprimare. Acest lucru a dus la crearea unor formate de documente, cum ar fi Adobe PDF (Portable Document Format) si PostScript, care au fost concepute pentru a pastra aspectul si formatarea documentelor pe diferite sisteme informatice si dispozitive de imprimare.

In anii '90 si 2000, dezvoltarea internetului si a World Wide Web a dus la crearea de noi formate de documente, cum ar fi HTML (Hypertext Markup Language), XML (Extensible Markup Language) si XHTML (Extensible Hypertext Markup Language). Aceste formate au fost concepute pentru a permite partajarea si accesarea cu usurinta a documentelor online si au stat la baza multor pagini web si documente online pe care le folosim astazi.

In prezent, documentele electronice sunt omniprezente si exista nenumarate formate de fisiere si aplicatii software care pot fi utilizate pentru a le crea, edita si partaja. De la simple documente de text la prezentari multimedia complexe, documentele electronice au revolutionat modul in care comunicam si impartasim informatii.

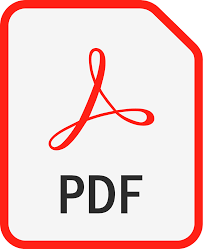
## Tipuri

Exista multe tipuri diferite de documente electronice, fiecare avand propriul format de fisier si propriul scop. Cateva dintre tipurile des folosite sunt:

Documente text: Acestea sunt documente simple care contin doar text, cum ar fi scrisori, memo-uri si rapoarte. Acestea sunt adesea create cu ajutorul unui software de procesare a textelor, cum ar fi Microsoft Word, si sunt salvate in formate de fisier precum DOCX sau RTF.

Foi de calcul (Spreadsheets): Aceste documente sunt utilizate pentru organizarea si analizarea datelor in format tabelar, cum ar fi situatiile financiare, listele de inventar si programele de proiect. Ele sunt adesea create cu ajutorul unui software precum Microsoft Excel si salvate in formate de fisier precum XLSX sau CSV.

Prezentari: Aceste documente sunt utilizate pentru a crea prezentari vizuale care includ text, imagini si elemente multimedia, cum ar fi cele audio si video. Acestea sunt adesea create cu ajutorul unui software precum Microsoft PowerPoint si sunt salvate in formate de fisier precum PPTX sau PDF.

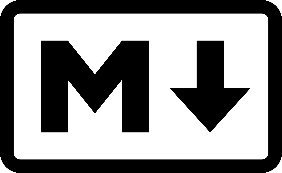
PDF-uri: PDF (Portable Document Format) este un format de fisier dezvoltat de Adobe care este utilizat pe scara larga pentru partajarea documentelor online. PDF-urile pot include text, imagini si elemente multimedia si pot fi vizualizate folosind o varietate de aplicatii software.

Carti electronice: Acestea sunt versiuni digitale ale cartilor care pot fi citite pe un computer sau pe un dispozitiv mobil. Ele sunt adesea create cu ajutorul unor programe specializate, cum ar fi Adobe InDesign, si sunt salvate in formate de fisier precum EPUB sau MOBI.

Imagini: Acestea sunt fisiere digitale care contin continut vizual static sau animat, cum ar fi fotografii, ilustratii si logo-uri. Acestea sunt adesea create cu ajutorul unor programe software precum Adobe Photoshop sau Illustrator si salvate in formate de fisier precum JPEG, PNG sau GIF.

Audio si video: Acestea sunt fisiere digitale care contin continut audio sau video, cum ar fi muzica, podcasturi si filme. Acestea sunt adesea create cu ajutorul unui software specializat precum Adobe Audition sau Premiere Pro si sunt salvate in formate de fisier precum MP3, WAV sau MP4.

Documente de proiectare: Acestea sunt documente utilizate in procesul de proiectare si dezvoltare a produselor si serviciilor. Aceste documente pot include diagrame, schemari, schite si desene. Ele sunt de obicei create folosind software-uri de proiectare asistata de calculator, cum ar fi AutoCAD sau SolidWorks.

Markdown: Markdown este un limbaj usor de marcare care este utilizat pentru a crea documente text simple care pot fi usor convertite in HTML sau in alte formate. Este utilizat in mod obisnuit pentru a scrie documentatie, articole de blog si alte tipuri de continut web. Fisierele Markdown sunt salvate cu extensii de fisiere precum .md sau .markdown.

LaTeX: LaTeX este un limbaj de tiparire care este utilizat pentru a crea documente complexe, in special in contexte academice si stiintifice. Este adesea utilizat pentru a crea rapoarte tehnice, lucrari de cercetare si carti. Fisierele LaTeX sunt salvate cu extensii de fisiere precum .tex.

Formulare: Acestea sunt documente digitale care includ campuri sau spatii goale pentru ca utilizatorii sa introduca informatii, cum ar fi formulare de cerere, sondaje si contracte. Acestea sunt adesea create cu ajutorul unui software precum Adobe Acrobat si sunt salvate in formate de fisier precum PDF.

OpenDocument: OpenDocument este un format de document cu sursa deschisa, conceput pentru a fi neutru fata de furnizor si independent de platforma. Este utilizat de o varietate de aplicatii software, inclusiv LibreOffice, si este salvat cu extensii de fisiere precum ODT pentru documente text, ODS pentru foi de calcul si ODP pentru prezentari.

E-mailuri: Acestea sunt mesaje digitale trimise si primite cu ajutorul unui software de e-mail sau al serviciilor de webmail. Acestea pot include text, imagini si atasamente si sunt adesea salvate in formate de fisiere precum EML sau MSG.

## Importanta documentelor electronice in societatea moderna

In era digitala, documentele electronice sunt omniprezente. Acestea sunt utilizate in toate domeniile, de la business la educatie si guvernare, si sunt stocate pe servere si dispozitive personale, in loc de medii fizice cum ar fi hartia si suporturile de stocare analogice. Din acest motiv, securitatea documentelor electronice a devenit o preocupare majora pentru toti cei care utilizeaza aceste tipuri de documente.

Tot mai multe companii aleg sa arhiveze electronic documentele interne datorita multiplelor beneficii pe care le ofera atat din punct de vedere al costurilor, cat si al timpului de regasire al documentelor.

Arhivarea electronica sustine companiile in realizarea unor economii semnificative, de spatiu si de timp si reduce riscul de pierdere a documentelor. Unele dintre beneficii pot fi:

* Cresteti productivitatea angajatilor

Potrivit unui studiu al International Data Corporation a fost dovedit faptul ca angajatii petrec intre 20% si 40% din timp cautand diferite acte si documente. Implementarea unei solutii de arhivare electronica a documentelor intr-o organizatie contribuie la cresterea productivitatii si eficientei angajatilor si la imbunatatirea relatiilor cu partenerii de afaceri. Automatizarea proceselor de lucru simplifica cautarea, preluarea si utilizarea datelor.

* Reducerea costurilor

Solutia de arhivare electronica a documentelor are numeroase beneficii ce contribuie la imbunatatirea modului de functionare al unei companii, precum si la economisirea timpului si banilor. Cercetarile Harvard Business Review indica faptul ca angajatii unei companii petrec circa 50% din timpul lor cautand informatii. Asta inseamna ca jumatate din timpul petrecut la birou de fiecare angajat este utilizat fara ca acesta sa fie productiv sau ca organizatia dumneavoastra ar fi cu 50% mai profitabila daca ar solutiona aceasta problema.

* Scurizarea accesului la documente

Multe companii inca ezita sa faca trecerea la arhivarea electronica a documentelor, punand la indoiala nivelul de siguranta si protectie al documentelor. Insa, exista multe modalitati de a proteja datele sensibile din documentele digitale, modalitati ce vor fi analizate in acest proiect.

Toate interactiunile cu un document arhivat electronic, spre exemplu accesari, vizualizari, transmiteri sunt inregistrate si contin informatii referitoare la data, ora si utilizator. Mai mult decat atat, documentele nu pot fi sterse din sistem de o persoana neautorizata sau inainte de depasirea termenului legal de pastrare, avand astfel o trasabilitate sigura si un istoric complet la nivel de document.

* Protejarea integritatii documentelor

Arhivarea documentelor in format fizic pierde teren in fata arhivarii electronice deoarece prima este expusa la potentiale pericole asociate cu gestionarea documentelor. Acestea pot fi arhivate gresit sau se pot deteriora fie din cauza modului in care au fost arhivate, fie din cauza accesarii repetate. Intr-o arhiva electronica se pastreaza o copie a documentului original, ce nu poate fi sters, pierdut sau expus unor factori exteriori care il pot deteriora, iar consultarea repetata nu va afecta integritatea acestuia.

In functie de tipul documentului, legea prevede diferite termene de pastrare pe categorii de documente, unele necesitand pastrarea pe o perioada indelungata de timp. Alegand arhivarea electronica a documentelor, legea este respectata fara a va teme de pagube cauzate de incendii sau inundatii. Astfel sunt reduse riscurile pierderii documentelor importante si de a suporta consecinte care nu pot fi evaluate din timp.

* Accesarea instanta a documentelor

Prin intermediul unei solutii de arhivare electronica se poate scana si arhiva orice tip de document, fie ca este vorba despre documente nestructurate, semistructurate sau structurate ca forma, tiparite, scrise de mana sau imagini. Toate documentele sunt disponibile imediat, ceea ce inseamna ca nu veti mai pierde timpul cu cautarea informatiilor si a documentelor in mai multe sisteme, pe server sau in arhive fizice, permitand personalului sa aloce timp si implicare in alte proiecte importante ale companiei. [6]

## Scopul si obiectivele proiectului

Proiectul analizeaza solutiile de securitate disponibile pentru documentele electronice si modul in care acestea pot fi utilizate pentru a asigura confidentialitatea si integritatea informatiilor.

Tema "Protectia si securitatea documentelor electronice" este una extrem de importanta in era digitala. Majoritatea documentelor sunt create, editate si pastrate in format electronic, ceea ce inseamna ca acestea sunt mai vulnerabile la atacuri cibernetice decat documentele traditionale in format fizic. Documentele electronice sunt din ce in ce mai frecvent utilizate, iar riscurile de securitate asociate cu acestea sunt in crestere.

Scopul principal al acestui proiect este sa ofere o intelegere profunda a metodelor de protectie si securitate a documentelor electronice si sa ofere solutii eficiente pentru a minimiza riscul de expunere la atacuri cibernetice. Sunt expuse diferite tipuri de atacuri cibernetice la care documentele electronice sunt expuse si va oferi o analiza a riscurilor asociate acestora. De asemenea, vor fi analizate diferitele metode de criptare si criptografie care sunt utilizate pentru a proteja informatiile electronice si pentru a asigura integritatea si autenticitatea acestora.

In ultimii ani, a crescut preocuparea pentru protejarea documentelor electronice intr-o varietate de contexte, inclusiv in domeniul juridic, medical, financiar si in afaceri. Aceasta crestere a preocuparii pentru securitatea informatiilor a dus la o cerere crescuta pentru tehnici si solutii de securitate a documentelor electronice, precum si pentru specialisti calificati in domeniul securitatii informatiilor.

Este important de subilinat faptul ca securitatea documentelor electronice nu este un proces static, ci unul dinamic. Aceasta necesita o abordare continua si o evaluare constanta pentru a asigura ca protectia ramane la un nivel adecvat, in conformitate cu noile amenintari si cu noile tehnologii.

Un alt aspect important al protectiei documentelor electronice este asigurarea legalitatii acestora. Documentele electronice trebuie sa fie valide din punct de vedere legal, iar aceasta valabilitate trebuie sa fie protejata. Este important ca documentele electronice sa fie semnate digital si sa fie certificate prin intermediul autoritatilor de certificare pentru a se asigura autenticitatea acestora.

In ceea ce priveste rolul protectiei si securitatii documentelor electronice in cadrul domeniului IT, acesta este un aspect cheie al securitatii informatiilor. Fara protejarea adecvata a documentelor electronice, acestea pot fi accesate si utilizate de catre persoane neautorizate, ceea ce poate duce la pierderea de informatii sensibile si la deteriorarea reputatiei unei companii.

Prin urmare, este important ca orice organizatie care utilizeaza documente electronice sa acorde o atentie deosebita protectiei si securitatii acestora. Prin implementarea unor masuri adecvate de securitate, organizatiile pot asigura protectia informatiilor lor si pot evita problemele care pot aparea ca urmare a accesului neautorizat la aceste informatii.

Asadar, proiectul va oferi o intelegere detaliata a importantei protectiei si securitatii documentelor electronice si va oferi solutii eficiente pentru a minimiza riscul de expunere la atacuri cibernetice. Prin abordarea acestei teme, vor fi subliniate si dezvoltate competente si puncte cheie in domeniul IT, care sunt extrem de valoroase in societatea actuala, din ce in ce mai dependenta de tehnologie.

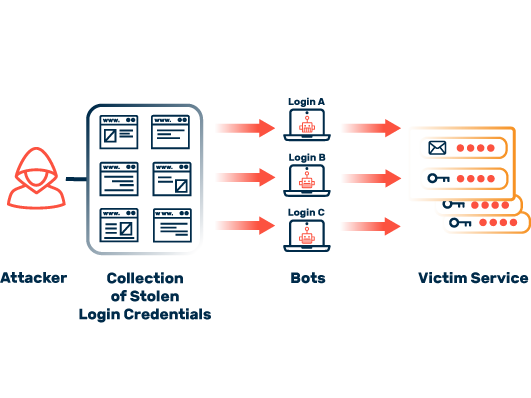
# Aprofundarea tematicii documentelor electronice

## Riscurile si amenintarile

### Accesul neautorizat

Accesul neautorizat este atunci cand cineva obtine acces la un site web, program, server, serviciu sau alt sistem folosind contul sau creditentialele unui utilizator ori alte metode. De exemplu, daca cineva continua sa ghiceasca o parola sau un nume de utilizator pentru un cont care nu-i apartine pana cand obtine accesul, acest lucru este considerat acces neautorizat.

Accesul neautorizat poate aparea, de asemenea, daca un utilizator incearca sa acceseze o zona a unui sistem pe care nu ar trebui sa o acceseze. Atunci cand incearca sa acceseze acea zona, i s-ar refuza accesul si ar putea vedea un mesaj de acces neautorizat.



\* atacator

\* serviciu victima

\* boti

(c) Myra

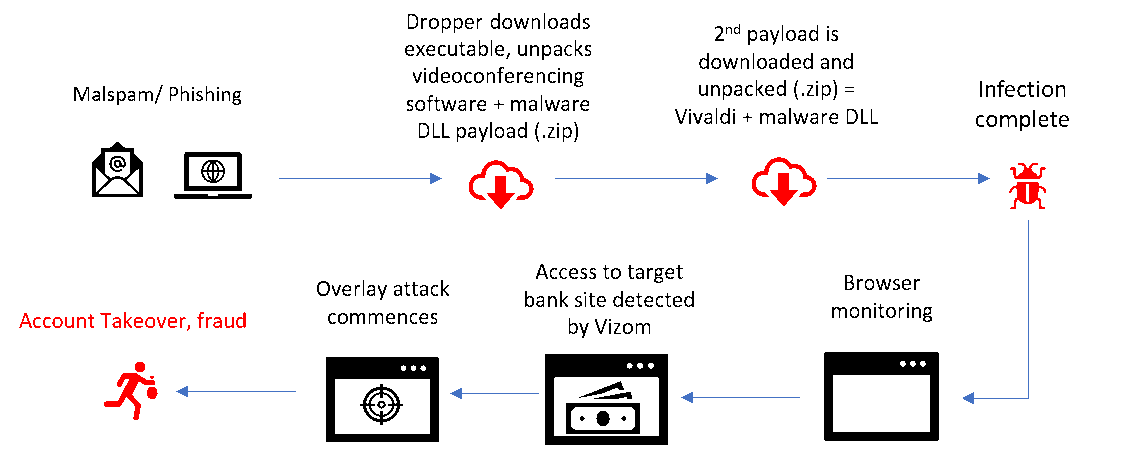
\* colectie de date autentificare furate

Unii administratori de sistem seteaza alerte care sa ii anunte atunci cand exista o incercare de acces neautorizat, astfel incat sa poata investiga motivul. Aceste alerte ajuta la impiedicarea hackerilor de a obtine acces la un sistem securizat sau confidential. Multe sisteme securizate pot, de asemenea, sa blocheze un cont in cazul unui numar prea mare de incercari de conectare esuate. [7]

### Virusi si malware

Amenintarea si riscul virusurilor si a malware-urilor asupra documentelor electronice sunt foarte mari in era digitala actuala.

Un virus informatic este un tip de malware care se ataseaza la un alt program (cum ar fi un document), care se poate reproduce si raspandi dupa ce o persoana il executa pentru prima data pe sistemul sau. De exemplu, prin e-mail, este trimis un atasament malitios, iar apoi virusul informatic se executa pe computer. Virusii sunt daunatori si pot distruge date, pot incetini resursele sistemului si pot inregistra apasarile de taste. [8]



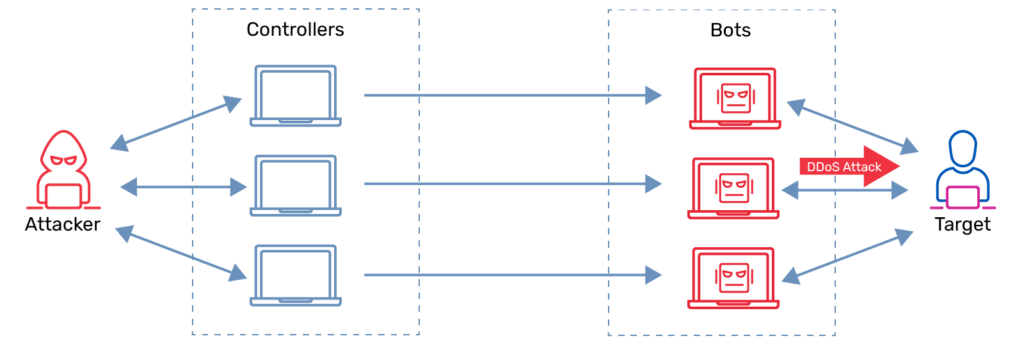
(c) threatpost

Atacurile cu virusuri si malware-uri pot fi devastatoare pentru documentele electronice, deoarece acestea sunt utilizate frecvent in afaceri, in guvernare si in comunicare personala. Documentele electronice pot fi compromise prin intermediul diferitelor tipuri de malware, cum ar fi virusuri, troieni, programe de spionaj, programe de ransomware etc.

Printre cele mai comune amenintari si riscuri ale virusurilor si malware-urilor pentru documentele electronice se regasesc:

* Pierderea de date: Atacurile cu virusuri si malware-uri pot determina pierderea sau deteriorarea documentelor electronice importante.
* Furtul de informatii personale: Malware-ul poate fi conceput pentru a colecta informatii despre utilizatori si a le trimite catre hackeri sau terti rau intentionati. Aceste informatii pot include parole, numere de carduri de credit si alte informatii sensibile.
* Santajul cu rascumparare: Ransomware-ul poate bloca accesul la documentele electronice si poate cere o rascumparare pentru a le elibera. Acest lucru poate fi costisitor si poate duce la pierderea de informatii vitale.
* Infectarea intregului sistem: Virusurile si malware-urile pot se pot raspandi in intregul sistem informatic, infectand si compromitand alte fisiere si programe.

### Atac cibernetic



\* controlere

\* boti

\* tinta

\* atacator

(c) iiTD

Atacurile cibernetice urmaresc sa deterioreze sau sa obtina control sau acces la documente si sisteme importante dintr-o retea de computere de firma sau personala.

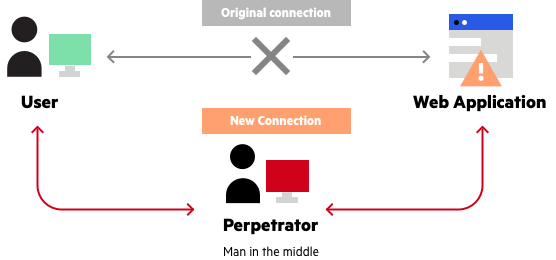
Atacurile cibernetice sunt distribuite de catre persoane sau organizatii pentru intentii politice, infractionale sau personale pentru a distruge sau a obtine acces la informatii clasificate.

Atacurile cibernetice sosesc in diverse forme prin intermediul retelelor si sistemelor de computere. Malware-ul si phishingul sunt doua exemple de atacuri cibernetice utilizate pentru a obtine control asupra datelor confidentiale de pe dispozitive electronice personale si de firma.

* Un atac DdoS (atacul distribuit de refuzare a serviciilor) este acela in care mai multe sisteme de computere atacate de hackeri vizeaza un site sau o retea si refuza activitatea utilizatorului pe acel site web sau retea. De exemplu, sute de ferestre pop-up, reclame si chiar un site care se defecteaza pot contribui la un atac DDoS pe un server compromis.
* Phishingul este actul de trimitere de e-mailuri frauduloase in numele companiilor renumite. Hackerii utilizeaza phishingul pentru a obtine acces la datele dintr-o retea personala sau de firma.
* Un atac de injectare SQL este cel in care un infractor cibernetic exploateaza software-ul, profitand de aplicatii (de exemplu, LinkedIn, Target) pentru a fura, a sterge sau a obtine control asupra datelor.
* Scriptarea intre site-uri (XSS) este atacul in care un infractor cibernetic trimite un link catre un site web care lanseaza spam sau este "injectat prin script" si acesta se deschide, livrand informatii personale catre respectivul infractor.
* Atacurile botnet sunt cele in care mai multe computere, in general dintr-o retea privata, sunt infectate cu virusi si alte forme de software rau intentionat, de exemplu, mesaje pop-up sau spam. [9]

### Atacurile "man-in-the-middle"

In momentul in care un utilizator acceseaza o pagina web, informatia este transmisa de la server catre computerul sau prin cabluri de mare viteza, routere si comutatoare de computere care contribuie la raspandirea internetului peste tot in lume. Un atac de tip man-in-the-middle este o procedura care permite atacatorului sa se interpuna intre utilizator si computerul cu care comunica, pentru a citi sau modifica acea conversatie. Aceasta procedura obisnuia sa fie foarte des intalnita inainte de trecerea masiva la protocolul HTTP-Secure si continua sa fie intalnita si in prezent, cu toate ca este mai greu de realizat. [10]



\* conexiune initiala

\* aplicatie web

\* utilizator

\* conexiune noua

(c) Imperva

\* omul din mijloc

### Expunerea accidentala sau intentionata

Expunerea accidentala sau intentionata a informatiilor din documentele electronice poate avea consecinte grave. Aceasta poate duce la compromiterea datelor personale sau de afaceri, pierderea de fonduri si a increderii clientilor, precum si la incalcarea legilor si regulamentelor privind confidentialitatea datelor.

Se poate intampla cand documentele electronice sunt trimise sau stocate in mod incorect. Spre exemplu, un angajat poate trimite un e-mail sensibil la adresa gresita sau poate incarca un document pe un server de stocare in cloud care nu a fost configurat corect pentru a proteja informatiile sensibile. Aceste erori pot fi facute din greseala si pot fi rezolvate prin formarea angajatilor si prin implementarea unor politici si proceduri clare de gestionare a datelor.

De asemenea, poate avea loc si prin intermediul angajatilor rau intentionati sau a partenerilor de afaceri care divulga informatii sensibile fara permisiunea companiei. Un exemplu cunoscut la nivel mondial este al lui Edward Snowden, un fost angajat al Agentiei Nationale de Securitate (NSA) din SUA, care a dezvaluit in 2013 o serie de documente clasificate care au aratat amploarea programelor de supraveghere in masa ale guvernului american.

### Scaderea perfromantei sistemului informatic

Ca risc reprezinta o situatie in care un sistem informatic sufera o reducere semnificativa a performantei sale, ceea ce poate duce la pierderea sau coruperea datelor, precum si la incapacitatea de a executa sarcinile importante.

Acest risc poate fi cauzat de o varietate de factori, cum ar fi erorile de programare, suprasolicitarea sistemului, virusii informatici sau problemele hardware. Scaderea performantei sistemelor informatice poate avea consecinte grave pentru organizatii sau indivizi, de aceea este important sa se ia masuri pentru a preveni si a proteja impotriva acestui risc.

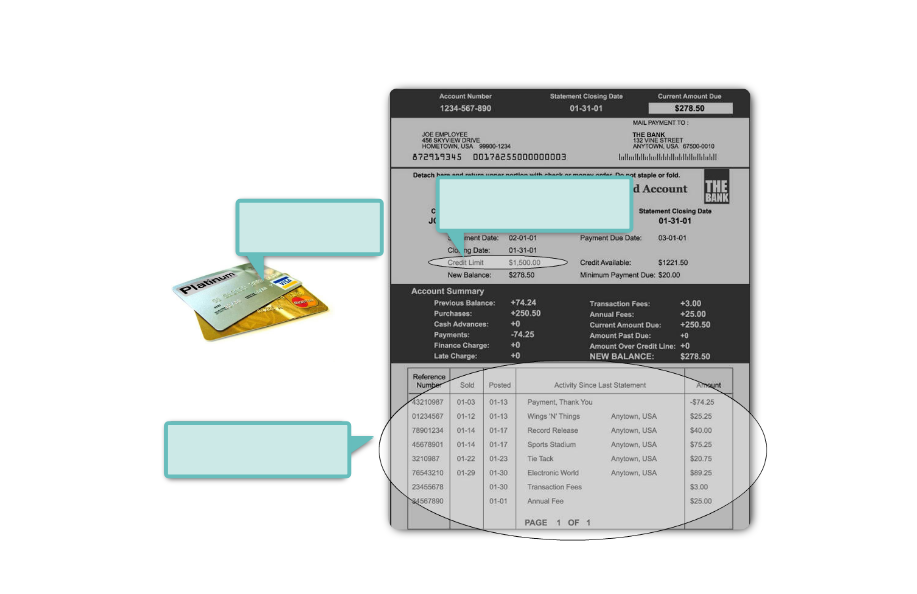
## Masuri de protectie si securitate pentru documentele electronice

### Autentificare si autorizare

Autentificarea si autorizarea sunt doua elemente esentiale in securitatea documentelor electronice. Autentificarea este procesul prin care sistemul verifica identitatea unui utilizator, in timp ce autorizarea se refera la permisiunile acordate utilizatorului.

Pentru autentificare sunt folositi anumiti factori ce pot fi clasificati in trei tipuri distincte:

* informatie pe care utilizatorul o cunoaste deja (inclusiv parolele) - siruri de caractere ce pot fi introduse de la tastatura etc.
* informatie existenta sub forma unui dispozitiv – autentificarea prin doui factori (2FA), smart card, token, card de memorie, inclusiv locatia fizica a utilizatorului.
* identitatea utilizatorului – o caracteristica anatomica a acestuia – amprente, timbru vocal, forma retinei sau a irisului, topologia palmei etc. Acest factor este in mod curent denumit factorul biometric. [11]



Comparatie practica

**Autorizatie**: cat de mult poti cheltui?

**Autentificare**: cine esti?

(c) Cisco

Pentru a proteja documentele electronice, este important sa se utilizeze metode puternice de autentificare si sa se configureze autorizarea cu atentie. De asemenea, este important sa se revizuiasca regulat permisiunile acordate utilizatorilor pentru a asigura o protectie continua a documentelor electronice.

### Criptare

Criptarea datelor presupune conversia unui text sau a datelor utilizate intr-un cod, numit si "text cifrat" sau "cod cifrat", care nu poate fi inteles de catre cei care nu detin cheia corecta. Scopul criptarii este de a permite trimiterea informatiilor relevante si, adesea, sensibile prin internet sau alte mijloace electronice fara ca persoanele neautorizate sa aiba acces la ele, de asemenea reprezentand o masura importanta de securitate pentru documentele electronice, deoarece acestea pot fi interceptate de hackeri sau alte persoane rau intentionate in timpul transmiterii lor prin retele de comunicatii. Pentru a putea fi utilizate, datele trebuie sa fie convertite inapoi in formatul lor original sau decriptate cu ajutorul unei chei pe care o detin doar utilizatorii autorizati.

Criptarea este necesara pentru protejarea datelor importante impotriva furtului sau a partajarii neautorizate. De exemplu, filmele folosesc managementul drepturilor digitale (DRM) pentru a preveni copierea ilegala, iar parolele de conectare la aplicatii sau site-urile web ale bancilor sunt criptate pentru a proteja informatiile financiare ale utilizatorilor.

Exista mai multe algoritme de criptare, cum ar fi AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), DES (Data Encryption Standard) si multe altele. Acestea sunt utilizate pentru a proteja diverse tipuri de date, de la parole si chei de criptare pana la documente importante si mesaje confidentiale.

Cu toate acestea, este important faptul ca in general, criptarea poate fi invinsa cu timp si efort suficiente, iar securitatea documentelor electronice nu se bazeaza exclusiv pe criptare. In plus, utilizarea incorecta a criptarii poate duce la vulnerabilitati de securitate. Prin urmare, este important sa se ia in considerare si alte masuri de securitate.

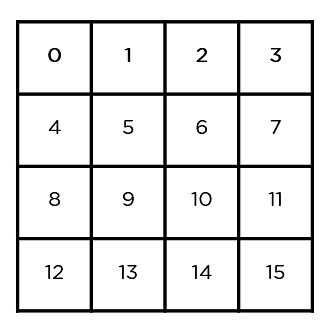
**Advanced Encryption Standard** [12]

AES este un standard de criptare a datelor adoptat pe scara larga si utilizat in intreaga lume. Este standardul federal utilizat de guvernul Statelor Unite si ofera o securitate si o protectie semnificative.

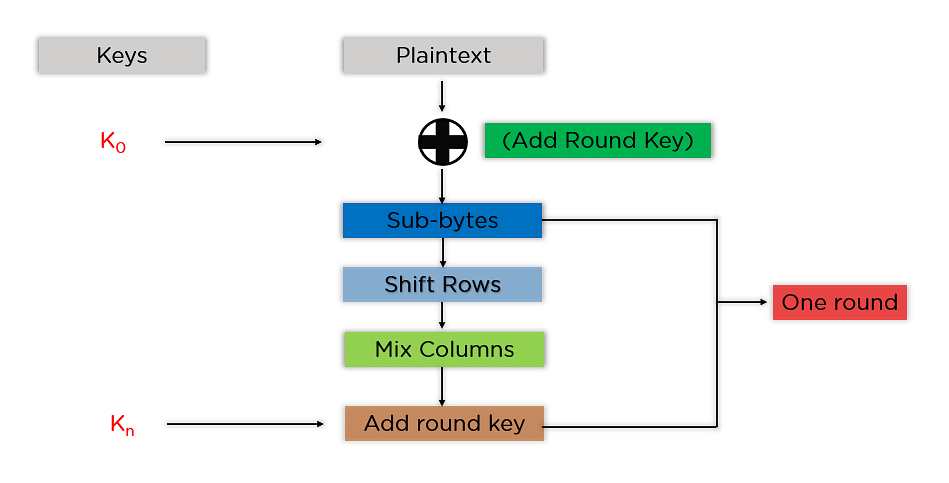
AES este un tip de criptare simetrica, care utilizeaza aceeasi cheie pentru a cripta si decripta datele. In esenta, atat expeditorul, cat si destinatarul au nevoie de aceeasi cheie pentru a decripta datele. Criptarea simetrica este mai rapida, desi este un pic mai putin sigura decat cea asimetrica.

*Principii teoretice:*

Deoarece un singur bloc are 16 octeti, o matrice 4x4 contine datele dintr-un singur bloc, fiecare celula contine un singur octet de informatie.

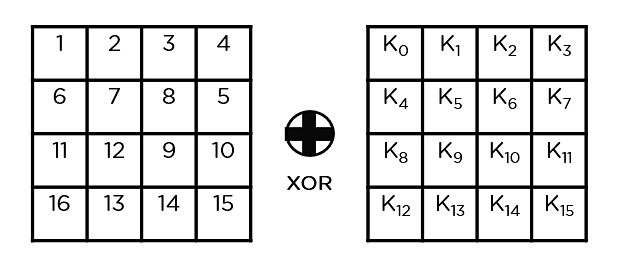


Matricea este cunoscuta sub numele de matrice de stare. In mod similar, cheia utilizata initial este extinsa in (n+1) chei, n fiind numarul de runde care urmeaza sa fie urmate in procesul de criptare. Astfel, pentru o cheie de 128 de biti, numarul de etape este de 16, numarul de chei care trebuie generate fiind de 10+1, ceea ce inseamna un total de 11 chei.

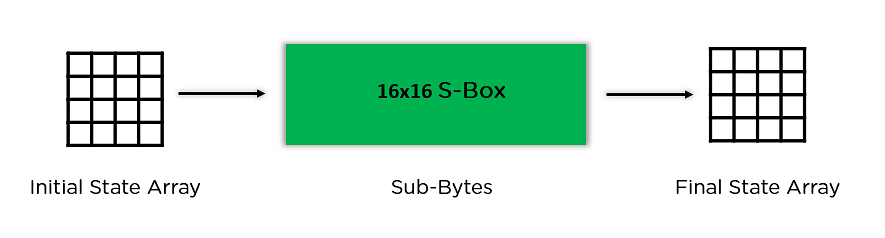


Pasii mentionati trebuie urmati pentru fiecare bloc in parte, in mod secvential. Dupa criptarea cu succes a blocurilor individuale, acestea se unesc pentru a forma textul cifrat final. Pasii sunt urmatorii:

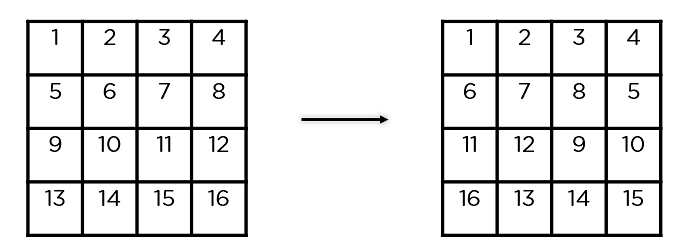
* Adaugarea cheii de runda: Se trec datele blocului stocate in matricea de stare printr-o functie XOR cu prima cheie generata (K0). Aceasta transmite matricea de stare rezultata ca intrare la pasul urmator.



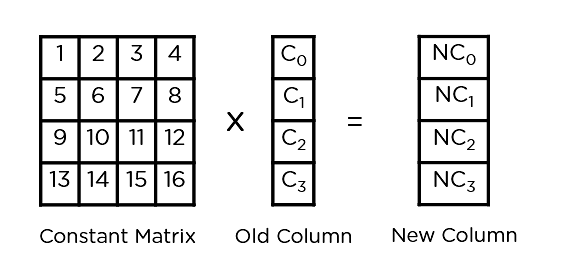
* Sub-Octeti: In aceasta etapa, se converteste fiecare octet al matricei de stare in hexazecimal, impartit in doua parti egale. Aceste parti sunt randurile si coloanele, mapate cu o caseta de substitutie (S-Box) pentru a genera noi valori pentru matricea de stare finala.



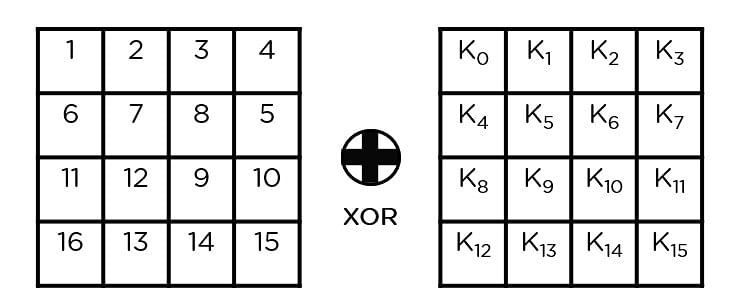
* Schimba randurile: Schimba elementele randurilor intre ele. Sare peste primul rand. Deplaseaza elementele din al doilea rand, cu o pozitie spre stanga. De asemenea, decaleaza elementele din al treilea rand cu doua pozitii consecutive spre stanga si decaleaza ultimul rand cu trei pozitii spre stanga.



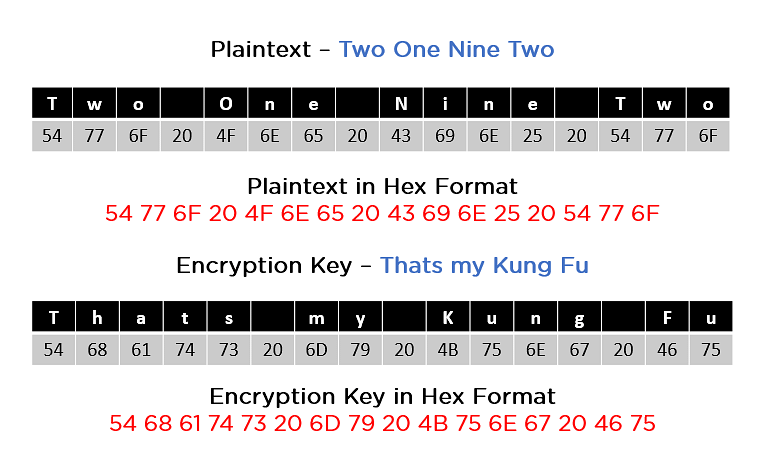
* Coloane mixte: Inmulteste o matrice constanta cu fiecare coloana din matricea de stari pentru a obtine o noua coloana pentru matricea de stari urmatoare. Odata ce toate coloanele sunt inmultite cu aceeasi matrice constanta, se obtine matricea de stare pentru pasul urmator. Aceasta etapa speciala nu trebuie efectuata in ultima runda.



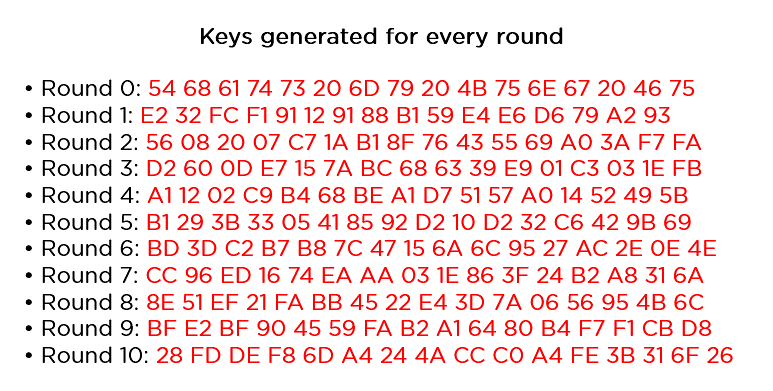
Adaugare Cheie de Runda: Cheia respectiva pentru serie este XOR-uita cu matricea starii obtinuta in pasul anterior. Daca aceasta este ultima serie, matricea de stare rezultata devine textul cifrat pentru blocul specific; in caz contrar, aceasta trece ca intrare pentru matricea de stare noua in seria urmatoare.



*Exemplu*:

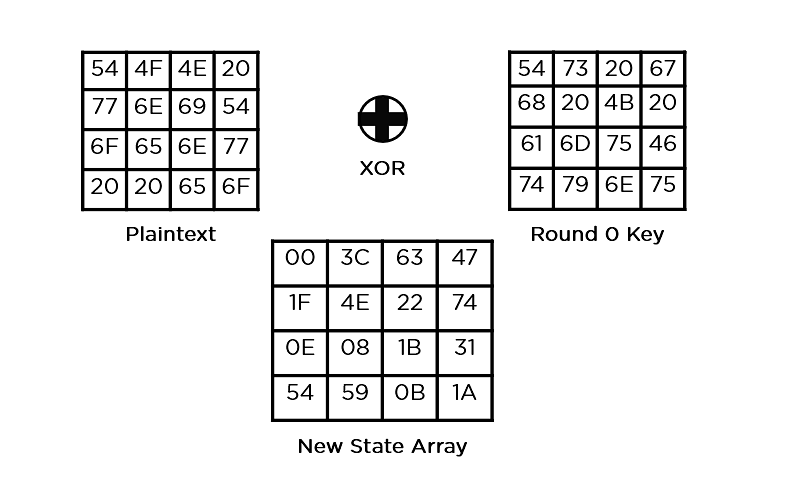


Textul in clar si cheia de criptare se convertesc in format hexazecimal inainte ca operatiile sa inceapa. In consecinta, se pot genera cheile pentru urmatoarele zece serii (runde).

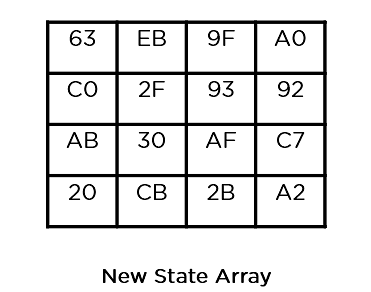


Este necesar sa se urmeze aceleasi pasi explicate mai sus, extragand secvential matricea de stare si trecand-o ca intrare la runda urmatoare. Pasii sunt urmatorii:

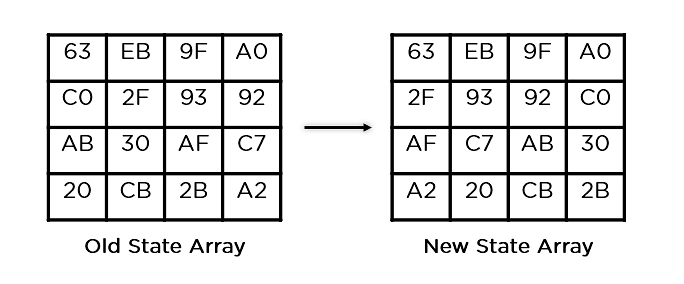
Adaugare Cheie Runda:



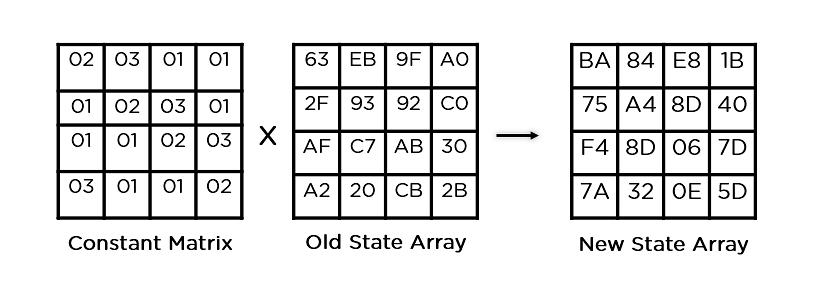
Elementele matricei de stare sunt trecute printr-un S-Box de 16x16 pentru a obtine o noua matrice de stare completa:



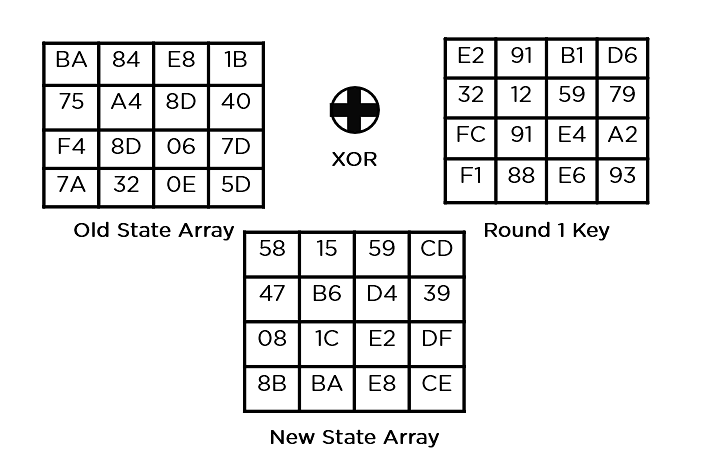
Deplasare Randuri:



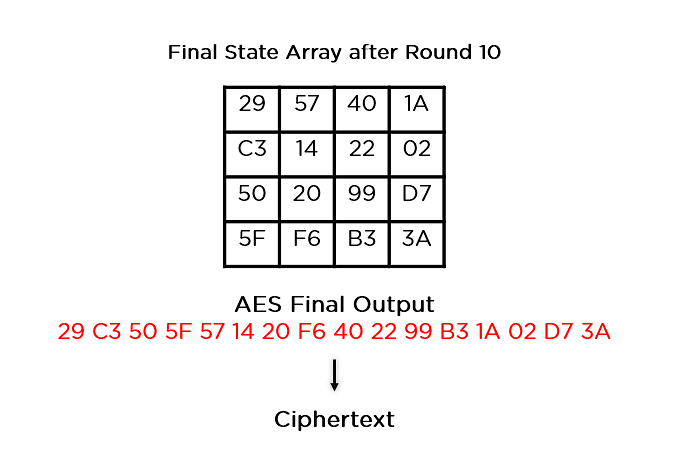
Combinare Coloane:



Adaugare Cheie Runda:



Matricea de stare este acum textul cifrat final pentru aceasta serie specifica. Devine intrarea pentru seria urmatoare. In functie de lungimea cheii, se repeta pasii pana cand se completeaza seria 10, dupa care se obtine textul cifrat final.



Standardul AES utilizeaza o dimensiune a blocului de 128 de biti.

In mare, 16 octeti inmultiti cu 8 biti ofera 128 de biti in fiecare bloc. Asadar, indiferent de dimensiunea cheii, dimensiunea blocului ramane aceeasi. De asemenea, AES a suferit multe atacuri, dar nu a fost inca spart.

AES-256 este cea mai sigura versiune, desi necesita o putere de calcul mai mare. Avand in vedere amenintarea iminenta a criptografiei post-cuantice, se considera ca AES-256 este un cod rezistent cuantic, ceea ce inseamna ca nu ar fi posibil ca dispozitivele, calculatoare cuantice sa poata sparga acest cod. [13]

|  |  |
| --- | --- |
| **Dimensiune** | **Combinatii posibile** |
| 1 bit | 2 |
| 2 biti | 4 |
| 4 biti | 16 |
| 8 biti | 256 |
| 16 biti | 65536 |
| 32 biti | 4.2 x 109 |
| 56 biti (DES) | 7.2 x 1016 |
| 64 biti | 1.8 x 1019 |
| 128 biti (AES) | 3.4 x 1038 |
| 192 biti (AES) | 6.2 x 1057 |
| 256 biti (AES) | 1.1 x 1077 |

Dimensiunile cheilor si combinatiile posibile corespunzatoare pentru a le sparge prin atac cu forta bruta.

Sursa: *https://www.atpinc.com/blog/what-is-aes-256-encryption*

Criptarea AES este un algoritm de criptografie simetrica. Procesul de criptare si de decriptare utilizeaza aceeasi cheie pentru ambele procese. AES a fost standardul pentru criptarea simetrica in ultimele cateva decenii si este inca utilizat pe scara larga in prezent pentru capacitatile sale de criptare sigura. AES este rapid si sigur, ceea ce il face o alegere populara pentru criptarea fisierelor si a altor date sensibile.

Caracterul deschis al standardului AES-256 face ca acesta sa fie unul dintre cele mai sigure standarde de criptare. Expertii in securitate cibernetica sunt in permanenta in cautare de potentiale vulnerabilitati, iar atunci cand este descoperita o vulnerabilitate, utilizatorii sunt notificati si se iau masuri pentru a rezolva problema.

Organizatiile trebuie sa protejeze si sa pastreze confidentialitatea datelor atunci cand acestea se afla in repaus si in miscare. Criptarea trebuie utilizata in ambele cazuri. Pentru datele in repaus, criptarea AES-256 este adesea cea mai buna optiune, in timp ce criptarea TLS (Transport Layer Security) creeaza tuneluri SSL (Secure Sockets Layer) pentru a proteja continutul privat. Datele private care necesita criptare includ informatii de identificare personala, informatii medicale protejate, inregistrari financiare si planuri strategice corporative de produse, marketing si vanzari. [14]

### SSL/TLS

Criptarea SSL (Secure Sockets Layer) si inlocuitorul sau mai modern si mai sigur, criptarea TLS (Transport Layer Security), protejeaza datele trimise pe internet sau intr-o retea de calculatoare. Acest lucru impiedica atacatorii (si furnizorii de servicii de internet) sa vizualizeze sau sa manipuleze datele schimbate intre doua noduri - de obicei, intre browserul web al unui utilizator si un server web/aplicatie. Majoritatea proprietarilor si operatorilor de site-uri web au obligatia de a implementa SSL/TLS pentru a proteja schimbul de date sensibile, cum ar fi parolele, informatiile de plata, formulare si alte informatii personale considerate private. [15]

TLS utilizeaza o combinatie de criptografie simetrica si asimetrica, deoarece aceasta ofera un bun compromis intre performanta si securitate atunci cand se transmit date in siguranta.

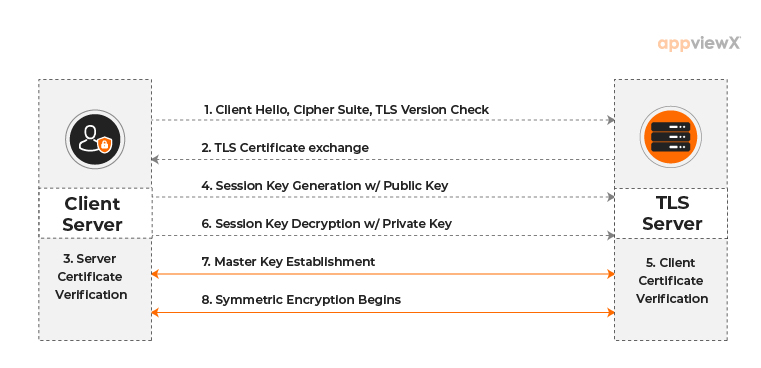
In cazul criptografiei simetrice, datele sunt criptate si decriptate cu o cheie secreta cunoscuta atat de expeditor, cat si de destinatar; de obicei, lungimea acesteia este de 128, dar de preferinta de 256 de biti (orice cifra mai mica de 80 de biti este considerata nesigura in prezent). Criptografia simetrica este eficienta din punct de vedere al calculului, dar existenta unei chei secrete comune inseamna ca aceasta trebuie partajata in mod sigur.

Criptografia asimetrica utilizeaza perechi de chei - o cheie publica si o cheie privata. Cheia publica este legata din punct de vedere matematic de cheia privata, dar, avand in vedere o lungime suficienta a cheii, nu este practic din punct de vedere computational sa se obtina cheia privata din cheia publica. Acest lucru permite ca expeditorul sa utilizeze cheia publica a destinatarului pentru a cripta datele pe care doreste sa i le trimita, dar aceste date pot fi decriptate numai cu ajutorul cheii private a destinatarului. [16]

TLS are urmatoarele avantaje:

* Continutul conexiunii ramane criptat, privat si complet securizat - si nu poate fi descifrat cu usurinta de catre actori rau intentionati.
* Conexiunea este realizata numai daca este fiabila - aceasta verificare a fiabilitatii face parte din comunicatiile TLS si este impusa prin schimbul unui cod de autentificare a mesajelor.
* Utilizarea certificatelor PKI si TLS asigura verificarea identitatii ambelor parti care comunica.

Atunci cand doua sisteme care utilizeaza TLS incearca sa se conecteze, fiecare sistem va face un efort pentru a verifica daca celalalt suporta TLS. Acest proces se numeste "TLS handshake" si ambele parti decid asupra versiunii TLS, algoritmului de criptare, suitei de cifrare etc. care vor fi utilizate in cadrul procedurii. Odata ce un handshake TLS a fost executat cu succes, ambele sisteme incep sa faca schimb de date pe o linie sigura. [17]



### Firewall si Antivirus

Firewall si antivirus-ul sunt doua tipuri de software de securitate utilizate pentru a proteja sistemele informatice impotriva atacurilor cibernetice.

Firewall-ul este un sistem de securitate care filtreaza traficul de internet care intra si iese dintr-o retea. Acesta poate fi implementat la nivelul hardware sau software. Firewall-ul poate bloca traficul care nu este permis, precum si conexiunile de la adrese IP suspecte. De asemenea, poate permite accesul doar la anumite servicii si porturi, in functie de politica de securitate a retelei ori pentru orice dispozitiv sau program care nu are permisiunea de a accesa reteaua. Acesta poate fi o componenta hardware sau software, care poate fi configurata pentru a bloca accesul la anumite porturi sau adrese IP.

Antivirusul este un software de securitate care detecteaza, impiedica si elimina amenintarile de securitate, cum ar fi virusii, malware-ul, ransomware-ul, spyware-ul si alte amenintari cibernetice de pe un sistem. Acesta poate fi configurat pentru a scana si pentru a detecta amenintari atunci cand fisierele sunt descarcate sau deschise si poate efectua scanari regulate ale sistemului pentru a identifica si elimina amenintarile.

Ambele solutii de securitate sunt importante intr-o strategie de securitate a retelei, deoarece fiecare abordeaza diferite tipuri de amenintari si ofera un nivel suplimentar de protectie.

In contextul protectiei si securitatii documentelor electronice, firewall-ul si antivirusul pot fi utilizate pentru a preveni atacurile cibernetice care pot afecta documentele electronice. Firewall-ul poate fi configurat pentru a bloca traficul nedorit, precum atacurile de tip DDoS (Distributed Denial of Service), care pot afecta functionarea sistemului de stocare si transfer de date. De asemenea, antivirusul poate detecta si elimina virusii si alte programe malware care pot afecta documentele electronice.

Este important ca aceste instrumente sa fie actualizate si sa fie configurate in mod corespunzator pentru a asigura protectia datelor si a informatiilor personale.

### VPN

O retea privata virtuala (VPN), este o conexiune criptata pe internet de la un dispozitiv la o retea. Conexiunea criptata ajuta la asigurarea transmiterii in siguranta a datelor sensibile. Aceasta impiedica persoanele neautorizate sa acceseze traficul si permite utilizatorului sa isi desfasoare activitatea la distanta. Tehnologia VPN este utilizata pe scara larga in mediile corporative. [18]

VPN-ul poate fi utilizat pentru a securiza documentele electronice prin crearea unui canal sigur de comunicare intre dispozitivul utilizatorului si serverul VPN. Acest lucru face posibila transmiterea de informatii sensibile din cadrul fisierelor fara a exista riscul ca acestea sa fie interceptate.

### Backup si recuperarea datelor

Backup-ul si recuperarea datelor sunt doua aspecte esentiale ale securitatii documentelor electronice.

Un backup este o copie a datelor importante care este stocata intr-o locatie alternativa, astfel incat sa poata fi recuperata in cazul in care este stearsa sau este corupta. Datele ar trebui sa fie copiate la un interval de timp determinat de frecventa cu care se schimba datele, de valoarea lor si de timpul necesar pentru efectuarea copiei de rezerva.

De exemplu, o companie cu inregistrari ale clientilor care se schimba frecvent poate face o copie de rezerva a datelor la fiecare cateva ore. Chiar si datele mai sensibile, cum ar fi inregistrarile bancare, pot fi stocate pe unitati RAID redundante care ajuta la protejarea datelor chiar si in cazul in care o unitate se defecteaza. [19]

Testele de backup si recuperare examineaza practicile si tehnologiile unei organizatii in materie de securitate si replicare a datelor. Scopul este de a asigura recuperarea rapida si fiabila a datelor in caz de nevoie. Procesul de recuperare a fisierelor de date salvate prin backup este cunoscut sub numele de restaurare a fisierelor.

Backup-urile datelor sunt printre cele mai importante componente de infrastructura din orice organizatie, deoarece ajuta la protejarea impotriva pierderilor de date. Copiile de rezerva ofera o modalitate de restaurare a fisierelor sterse sau de recuperare a unui fisier atunci cand acesta este suprascris din greseala.

Intreprinderile fac de obicei copii de rezerva ale datelor cheie pe dispozitive de backup dedicate. Software-ul de backup - fie ca este integrat in dispozitive, fie ca ruleaza pe un server separat - gestioneaza procesul de copiere a datelor pe dispozitivele de disc. Software-ul de backup gestioneaza procese precum deduplicarea datelor, care reduc spatiul fizic necesar pentru stocarea datelor. De asemenea, software-ul de backup aplica politici care guverneaza frecventa de backup a anumitor date, numarul de copii efectuate si locul unde sunt stocate copiile de rezerva.

Sistemele efectueaza o copie de rezerva completa initiala pe disc, iar apoi efectueaza copii de rezerva incrementale la fiecare cateva minute, pe masura ce datele sunt create sau modificate. Aceste tipuri de copii de rezerva pot proteja atat datele structurate - datele stocate pe un server de baze de date - cat si datele nestructurate sau datele din fisiere.

Desi unele produse de backup inca folosesc servere de backup separate, furnizorii de backup trec din ce in ce mai mult la dispozitive integrate de protectie a datelor. Un dispozitiv integrat de date este, in esenta, un server de fisiere dotat cu HDD-uri si software de backup. Aceste dispozitive de stocare a datelor de tip plug-and-play includ adesea functii automatizate de monitorizare a capacitatii discurilor, stocare extensibila si biblioteci de benzi preconfigurate. De asemenea, pot sa ofere platforme de backup care se bazeaza pe utilizarea sistemelor hiperconvergente. Aceste sisteme constau in colectii de servere standardizate care au fost grupate impreuna si care gestioneaza in mod colectiv procesele legate de backup. Unul dintre principalele beneficii ale sistemelor hiperconvergente este faptul ca sunt usor de scalat.

Unitatile SSD (Solid-State Drive) sunt rareori folosite pentru backup-ul datelor din cauza problemelor legate de pret si de rezistenta. Unii furnizori de solutii de stocare includ SSD-urile ca instrument de cache sau de ierarhizare pentru gestionarea scrierilor in matricele bazate pe disc. Acest lucru este deosebit de comun in sistemele hiperconvergente. Datele sunt initial stocate in memoria cache in memoria flash si apoi scrise pe disc. Pe masura ce furnizorii lanseaza SSD-uri cu o capacitate mai mare decat cea a unitatilor de disc, unitatile flash ar putea fi utilizate pentru backup.

Sistemele de stocare primare au capacitati de backup incorporate mai bune, cum ar fi protectia RAID si replicarea snapshot-urilor. Cu toate acestea, backup-ul stocarii primare poate fi costisitor si nu are functii de indexare.

Backup-ul local copiaza datele pe unitati externe sau sisteme cu banda magnetica, de obicei aflate in apropierea centrului de date. Ofera o securitate mai buna a retelei si backup mai rapid cu mai mult control asupra accesului la date.

Backup-ul offline sau la rece (cold), este similar cu backup-ul local, dar este adesea folosit pentru baze de date. Necesita timp de inactivitate, deoarece baza de date este deconectata de la retea in timpul backup-ului.

Backup-ul off-site implica transmiterea datelor catre o locatie remote, cum ar fi un centru de date secundar sau un serviciu de stocare in cloud. Stocarea in cloud devine din ce in ce mai populara datorita costului redus si a scalabilitatii, dar utilizatorii trebuie sa ia masuri pentru a asigura securitatea datelor.

Stocarea in cloud este impartita in trei tipuri: publica, privata si hibrida. Stocarea in cloud publica implica trimiterea datelor catre un furnizor de servicii cloud, in timp ce stocarea in cloud privata implica backup-ul datelor catre servere din interiorul firewall-ului companiei. Stocarea in cloud hibrida utilizeaza atat stocarea locala, cat si cea remote.

Mai multe companii care ofera solutii de backup permit aplicatiilor locale sa fie backup-uite intr-un cloud privat, extinzand astfel centrul fizic de date al clientului. Acest proces poate permite, de asemenea, recuperarea in caz de dezastru ca serviciu, permitand aplicatiilor sa se recupereze in caz de dezastru si sa revina ulterior. [20]

Recuperarea datelor este procesul invers al backup-ului si implica restabilirea datelor pierdute sau deteriorate. Recuperarea datelor este un aspect esential al securitatii si protectiei documentelor electronice. In cazul in care datele electronice sunt pierdute sau deteriorate, recuperarea acestora poate fi o sarcina dificila. Exista insa mai multe modalitati de a realiza recuperarea documentelor electronice.

* Una dintre cele mai eficiente modalitati de recuperare a documentelor electronice este de la backup-ul realizat anterior. Acest lucru implica restabilirea datelor pierdute sau deteriorate dintr-un backup anterior care a fost pastrat intr-un mediu sigur si accesibil.
* In cazul in care backup-ul nu a fost realizat sau nu este disponibil, exista inca o serie de optiuni pentru recuperarea datelor. In unele cazuri, datele pot fi recuperate direct de la dispozitivul original, prin utilizarea unor programe specializate de recuperare a datelor. Aceste programe utilizeaza algoritmi avansati pentru a analiza si recupera datele deteriorate sau pierdute. Cu toate acestea, utilizarea acestor programe poate fi costisitoare si nu exista garantii pentru succesul recuperarii datelor.
* In cazurile mai grave, cand datele sunt pierdute in mod permanent, exista servicii specializate care pot ajuta la recuperarea datelor pierdute sau deteriorate. Aceste servicii pot fi costisitoare si nu pot garanta succesul in recuperarea datelor.

In general, este important sa se realizeze backup-ul datelor si sa se verifice regularitatea acestuia, astfel incat in cazul unui incident sa se poata recupera datele pierdute. De asemenea, este important sa se ia in considerare diferitele optiuni de stocare si recuperare a documentelor electronice.

### Protejarea documentelor cu o parola

Blocarea documentelor cu parola este o metoda de securizare a informatiilor personale sau confidentiale care sunt stocate in aceste formate de fisier. Atunci cand un document este blocat cu o parola, numai persoanele care cunosc parola pot accesa si vizualiza continutul documentului.

In Word, Excel sau PowerPoint, fisierul care trebuie protejat cu o parola poate fi deschis, iar apoi trebuie sa fie selectata optiunea Fisier si Info. In partea superioara a listei ar trebui sa fie afisata optiunea Protejare. Este necesar sa se faca clic pe acel buton si sa se aleaga optiunea Criptare cu parola (Encrypt with Password) pentru a introduce parola.

Parolele pot avea pana la 15 caractere si sunt sensibile la majuscule si minuscule, asa ca este necesara o reverificare a datelor introduse. In cazul pierderii parolei, accesul in acel document nu va mai putea fi facut. [21]

Toate fisierele Office (Office 2016 si versiunile ulterioare) protejate cu parola sunt criptate cu AES 256 de biti. Office 2010 si versiunile anterioare utilizeaza AES pe 128 de biti. Versiunile mai vechi ale Microsoft Office utilizeaza un algoritm de criptare proprietar.

Pentru restrictionarea accesului la un document Word, utilizarea unei parole puternice pentru protejarea acestuia poate fi la fel de eficienta ca orice alt tip de criptare cu parola. In cazul in care parola este necunoscuta, atacatorii ar trebui sa foloseasca un software specializat de eliminare a parolei pentru a incerca sa o sparga.

Cu toate acestea, pentru a impiedica partajarea neautorizata a unui document Word prin blocarea acestuia cu o parola, nu este foarte sigura, deoarece un utilizator autorizat poate partaja parola cu altii sau pur si simplu o poate elimina.

In ceea ce priveste restrictionarea editarii in Word, securitatea poate fi usor de ocolit si, prin urmare, poate constitui o pierdere de timp sa se incerce restrictionarea editarii in acest mod. Aceasta optiune permite utilizatorilor sa vizualizeze un document Microsoft Word, dar nu sa il editeze. Cu toate acestea, nu impiedica utilizatorii sa copieze continutul intr-un alt document Word, sa il salveze intr-un alt format sau sa il tipareasca pe un driver de fisiere. [22]

PDF-urile pot fi, de asemenea, protejate prin parola pentru a restrictiona vizualizarea continutului doar pentru anumiti utilizatori sau pot fi securizate prin modificarea setarilor de permisiune pentru a impiedica modificarea continutului si imprimarea fisierelor.

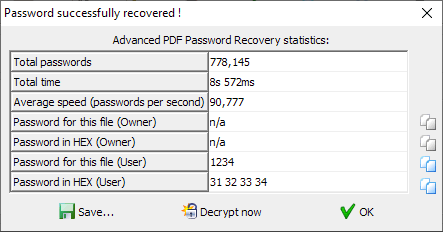
Adobe are doua niveluri de securitate pentru a proteja un PDF cu parola:

Parola documentului (Document open password): Denumita si parola utilizatorului sau parola proprietarului, aceasta controleaza cine poate deschide documentul PDF. Utilizatorul are nevoie de parola specificata si corecta pentru a deschide documentul.

Parola de permisiune (Permissions password): Cunoscuta si sub numele de parola principala, aceasta parola controleaza ceea ce pot face utilizatorii cu un document - daca il pot edita si imprima etc. Atunci cand este setata o parola de permisiune, destinatarii documentului nu sunt obligati sa introduca parola pentru a deschide documentul. Cu toate acestea, in cazul in care controalele de restrictionare a editarii trebuie resetate sau modificate, parola de permisiune trebuie sa fie tastata.

In cazul in care creatorul documentului PDF securizeaza fisierul PDF cu ambele tipuri de parole, documentul poate fi deschis cu oricare dintre parole. Cu toate acestea, pentru ca utilizatorul sa modifice caracteristicile restrictionate, trebuie introdusa parola de permisiune.

Utilizarea de parole pentru securizarea fisierelor PDF poate sa nu asigure suficienta protectie, deoarece acestea pot fi usor sparte cu ajutorul numeroaselor instrumente de spargere a parolelor si crackerelor de parole pentru PDF-uri (software-uri de recuperare a parolelor PDF) disponibile pe internet. Fisierele PDF care sunt protejate prin parola pot fi usor sparte daca se utilizeaza parole slabe.



(c) Locklizard

Exista diferite plugin-uri care permit protejarea unui fisier PDF cu Acrobat si monitorizarea utilizarii acestuia, dar acestea reprezinta de obicei un risc de securitate. Majoritatea acestora necesita activarea JavaScript-ului in document pentru a functiona sau dezactivarea securitatii in document, ceea ce poate expune utilizatorii la programe malware.

In ceea ce priveste fisierele, parolele documentului (de deschidere) sunt criptate cu cifrul de flux RC4. Parolele de permisiuni sunt stocate in PDF-ul in sine si nu utilizeaza criptare - se bazeaza in schimb pe aplicatiile de citire PDF pentru a respecta parola. [23]

Este important de subliniat ca blocarea unui document cu o parola nu garanteaza securitatea completa a informatiilor continute in acel document. In cazul in care parola este compromisa sau accesul neautorizat este obtinut prin alte mijloace, informatiile continute in documentul respectiv pot fi in continuare expuse riscurilor de securitate.

### Protectia datelor personale si a confidentialitatii

Protectia datelor personale si a confidentialitatii este o preocupare majora in societatea moderna, mai ales in contextul utilizarii documentelor electronice.

Exista numeroase reglementari si legi care se ocupa de protectia datelor personale in documentele electronice, inclusiv Regulamentul General privind Protectia Datelor (GDPR) si Directiva privind protectia datelor personale (DPD).

GDPR stabileste cerintele detaliate pentru companii si organizatii in ceea ce priveste colectarea, stocarea si gestionarea datelor cu caracter personal. Se aplica atat in cazul organizatiilor europene care prelucreaza datele cu caracter personal ale cetatenilor din UE cat si in cazul organizatiilor din afara UE care vizeaza cetateni din UE. [24]

Pentru a proteja datele personale in documentele electronice, acestea trebuie stocate intr-un mediu sigur si protejat prin parole si criptare. Accesul la aceste date trebuie limitat numai la persoanele autorizate, iar o procedura clara de gestionare a documentelor trebuie stabilita.

Transferul de date personale trebuie sa fie efectuat numai prin canale sigure si protejate pentru a se evita accesul neautorizat. Transferul prin email trebuie evitat pentru a preveni interceptarea.

Este important sa se stearga datele personale care nu mai sunt necesare. Este important sa se stabileasca o procedura clara pentru stergerea datelor personale, astfel incat acestea sa nu fie accesibile dupa ce au fost eliminate.

Pentru a proteja datele personale in documentele electronice, este important sa se ofere formare personalului cu privire la importanta protejarii datelor personale si a confidentialitatii. Personalul trebuie sa fie constient de politica de securitate si sa respecte regulile si procedurile stabilite.

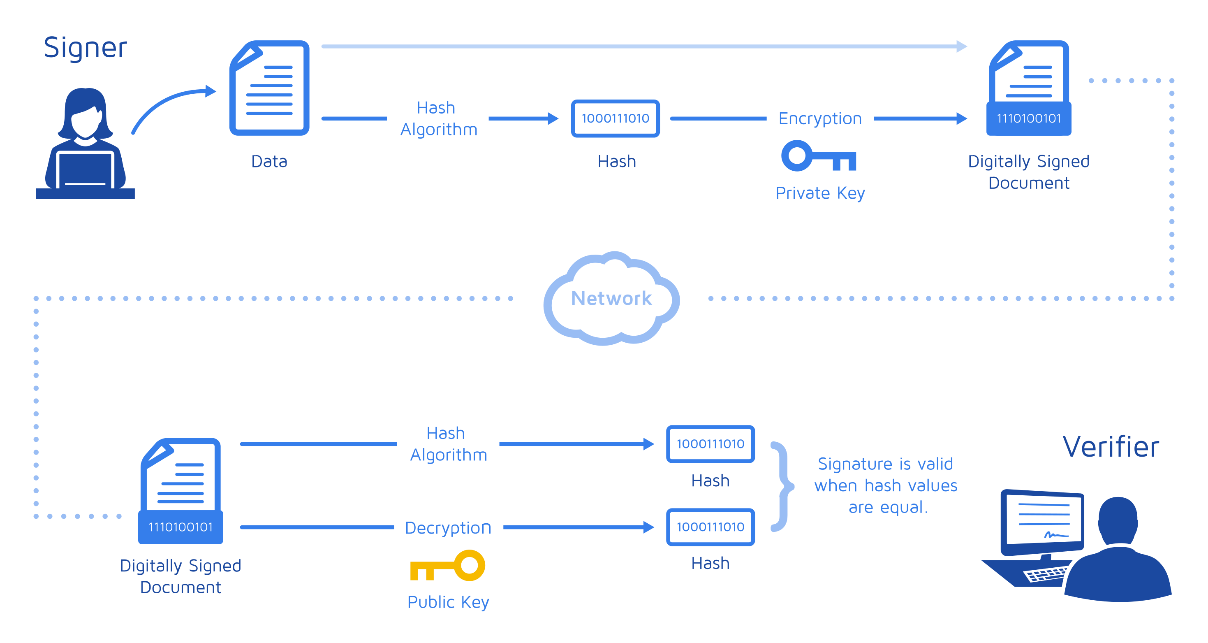
### Semnatura electronica si digitala

O semnatura digitala este un tip specific de semnatura care este sustinuta de un certificat digital, oferind dovada identitatii utilizatorului. Semnaturile digitale sunt recunoscute ca fiind un tip mai sigur de semnatura electronica, deoarece sunt legate criptografic de documentul semnat si pot fi verificate. Atunci cand este folosit un certificat digital obtinut de la o terta parte de incredere pentru a semna electronic, semnatura digitala rezultata este practic imposibil de falsificat. De asemenea, ofera dovezi puternice privind identitatea semnatarului, faptul ca documentul semnat nu a fost modificat si ca semnaturile sunt valide.

Asemanator unui pasaport in format electronic, o identitate digitala (sau ID digital) furnizeaza o proba puternica ca utilizatorul este autentic atunci cand semneaza electronic un document, fiind similara cu un pasaport in format electronic. Fiecare ID digital este sustinut de un certificat digital emis de o terta parte de incredere, cum ar fi o banca sau guvernul, dupa ce identitatea utilizatorului a fost verificata in mod exhaustiv. Utilizarea unui ID digital pentru a autentifica identitatea si a aplica o semnatura digitala in timpul procesului de semnare a documentului ofera un nivel mai ridicat de asigurare ca utilizatorul a fost de acord cu termenii enumerati si a autorizat semnatura pe un anumit document. [25]

O semnatura electronica este un termen generic pentru a reprezenta un consimtamant sau o aprobare. Poate fi o imagine de semnatura, desenata, apasata pentru a intra sau un simbol pentru a verifica un document. Ea nu este intotdeauna insotita de o dovada de identitate: Oricine ar putea incarca o imagine a unei semnaturi, iar aceasta nu are autoritatea necesara pentru a valida autenticitatea semnatarilor. [26]

Semnaturile digitale se bazeaza pe cheile publice si private. Aceste chei trebuie protejate pentru a asigura securitatea si a evita falsificarea sau utilizarea malefica. Atunci cand se trimite sau se semneaza un document, este necesara asigurarea ca documentele si cheile sunt create in siguranta si ca se folosesc chei valide. Autoritatile de Certificare (CA), un tip de Furnizor de Servicii de Incredere, sunt organizatii care au fost larg acceptate ca fiind de incredere pentru asigurarea securitatii cheilor si pentru a furniza certificate digitale necesare. Atat entitatea care trimite documentul, cat si destinatarul care il semneaza, trebuie sa fie de acord sa utilizeze o anumita CA. [27]



(c) DocuSign

### Politici si proceduri de securitate in cadrul unei companii

Politicile si proceduri de securitate sunt esentiale pentru protejarea documentelor electronice si a altor informatii sensibile. Acestea constau intr-un set de reguli, proceduri si practici de lucru care trebuie respectate de catre toti angajatii si colaboratorii unei organizatii.

Pentru a fi eficiente, politici si proceduri de securitate trebuie sa acopere o gama larga de aspecte, precum:

Accesul la date: se pot defini reguli privind accesul la documentele electronice, inclusiv cine are permisiunea sa le acceseze, cand si cum pot fi accesate si daca este necesara autorizarea suplimentara pentru a le accesa.

Protejarea parolelor: se pot defini reguli si proceduri pentru crearea si protejarea parolelor, cum ar fi durata de valabilitate, lungimea si complexitatea acestora.

Protectia dispozitivelor mobile: se pot defini reguli privind utilizarea dispozitivelor mobile si protectia datelor stocate pe acestea, cum ar fi folosirea de parole, criptarea datelor si blocarea dispozitivelor in caz de pierdere sau furt.

Utilizarea e-mailului: se pot defini reguli privind utilizarea e-mailului pentru a preveni trimiterea de informatii sensibile catre destinatari gresiti sau neautorizati.

Politici privind transferul de date: se pot defini reguli si proceduri pentru transferul de date intre dispozitive sau in afara organizatiei, inclusiv utilizarea de software securizat pentru a cripta si proteja datele.

Protectia impotriva virusilor si a altor amenintari cibernetice: se pot defini reguli privind utilizarea software-ului antivirus si firewall-ului pentru a preveni accesul neautorizat la datele organizatiei si pentru a proteja impotriva virusilor si a altor amenintari cibernetice.

Monitorizarea si auditarea: se pot defini reguli si proceduri pentru monitorizarea si auditarea utilizarii datelor organizatiei pentru a preveni utilizarea neautorizata si pentru a detecta si preveni eventualele incalcari ale securitatii.

In general, politici si proceduri de securitate sunt esentiale pentru protejarea datelor organizatiei si a altor informatii sensibile. Acestea trebuie sa fie actualizate regulat pentru a se adapta la noile amenintari cibernetice si la evolutia tehnologica.

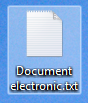
### Exemple aplicatii

In sensul documentelor electronice, se pot folosi diverse aplicatii cu mijloace diferite pentru protectie si securizare, fie individuala ori corporativa:

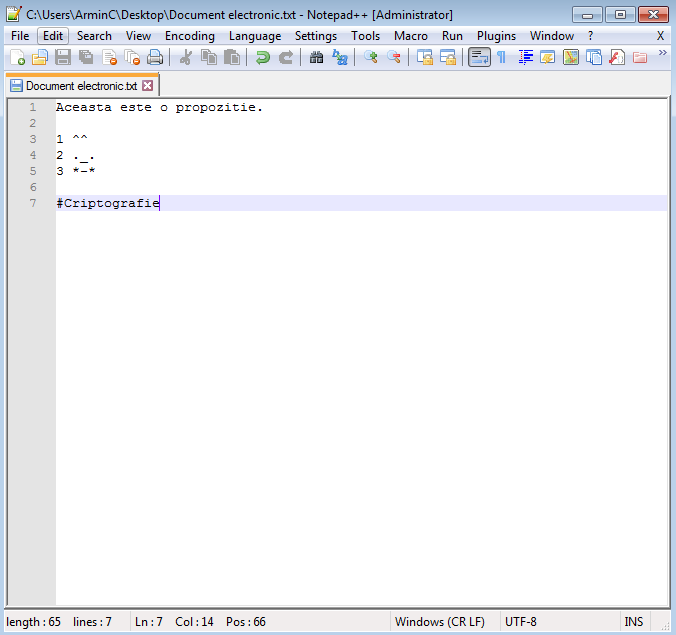
* Antivirus si software anti-malware, cum ar fi Kaspersky, Bitdefender, Norton, Sophos, Defender.
* Software de criptare a fisierelor, cum ar fi Cryptomator, Picocrypt, VeraCrypt, AxCryptm BitLocker, LUKS, hat.sh.
* Platforme de gestiune a documentelor si colaboare, cum ar fi Dropbox Business, Google Drive, Microsoft OneDrive, Box, MEGA, OnionShare.
* Aplicatii de securitate a retelei si VPN, cum ar fi IVPN, Mullvad, Proton VPN.
* Managere de parole: Bitwarden, 1Password, Psono, KeePassXC.
* Suite de securitate endpoint si programe de gestionare a vulnerabilitatilor, cum ar fi Microsoft Defender for Endpoint, Bitdefender GravityZone, KasperskyEndpoint, Sophos Endpoint Protection, Symantec Endpoint Protection.

### Lucru practic

In acest exemplu se va incerca criptarea unui document electronic cu formatul standard .txt.

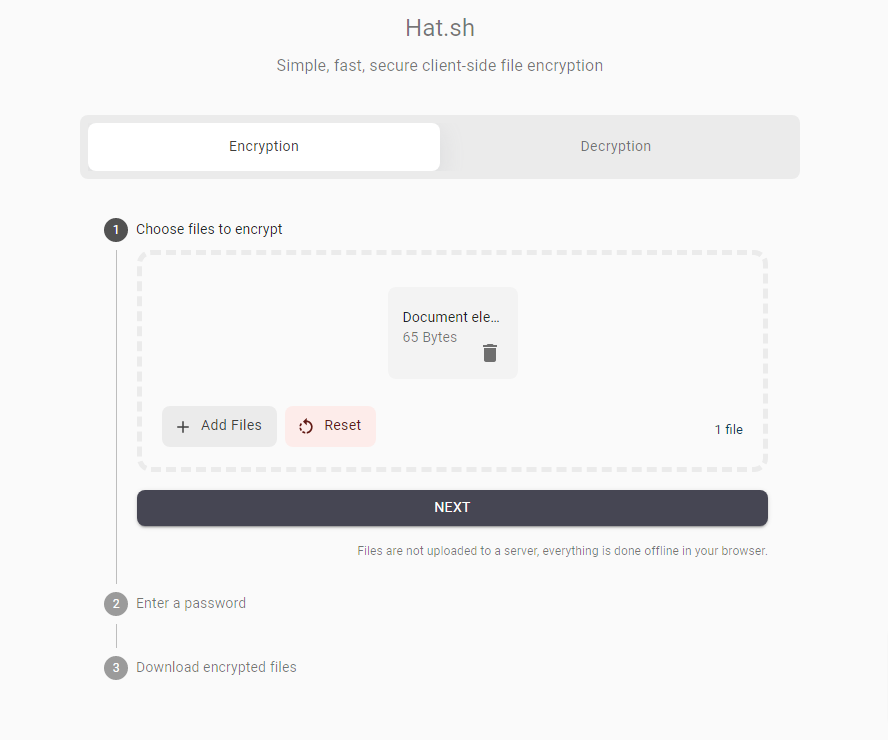


S-a creat fisierul **Document eletronic.txt**.

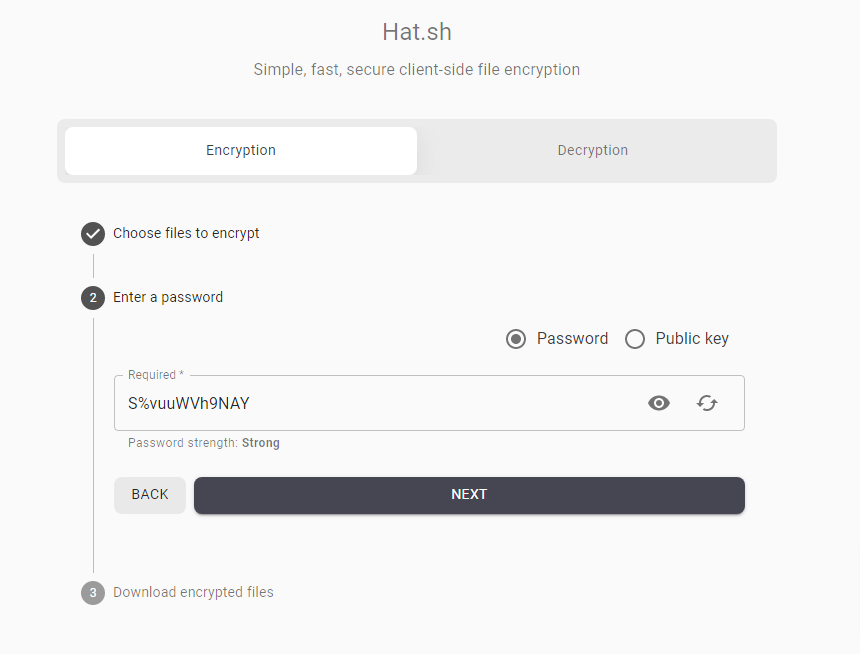


I s-a **atribuit un text** format din diverse caractere: litere, cifre si simboluri.

Pentru **criptare**, se foloseste **Hat.sh**, o aplicatie web care ofera criptarea securizata a fisierelor locale in browser, ce utilizeaza algoritmi criptografici moderni cu criptare/decriptare secventiala AEAD pe bucati.



Fisierul a fost **selectat**.



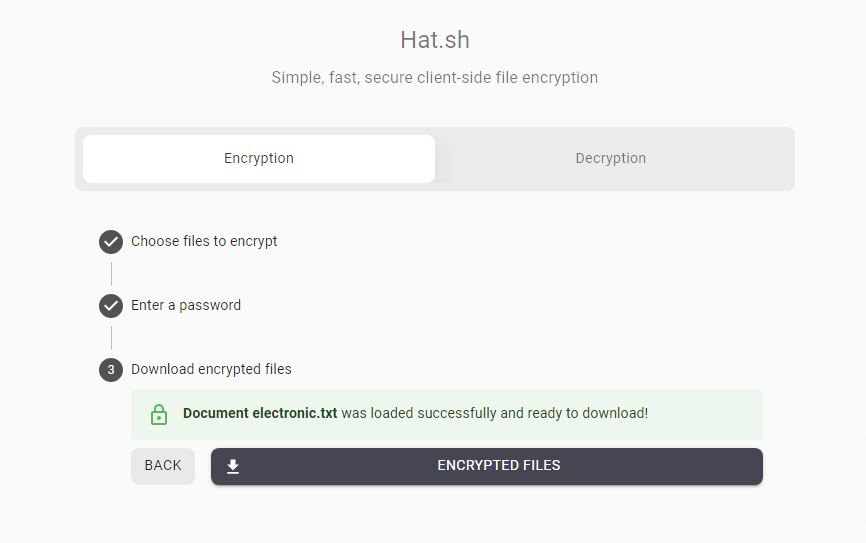
Se va selecta metoda de securizare. Acestea sunt fie prin **parola** sau prin **cheie publica**.

Tipul de *securitate* utilizat este:

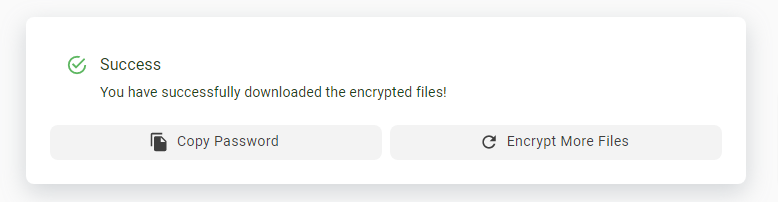
**XChaCha20-Poly1305** - pentru criptarea simetrica.

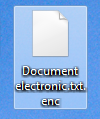
**Argon2id** - pentru derivarea cheii pe baza parolei.

**X25519** - pentru schimbul de chei.

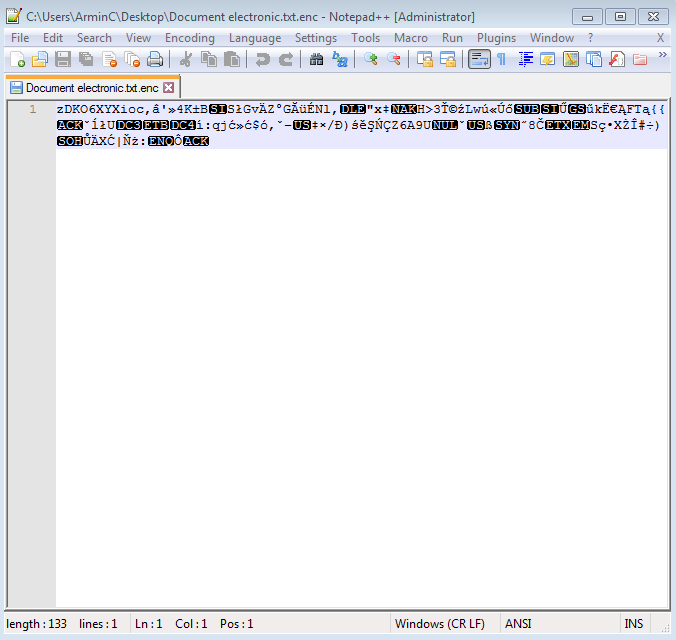


Fisierul a fost **criptat** si poate fi salvat.

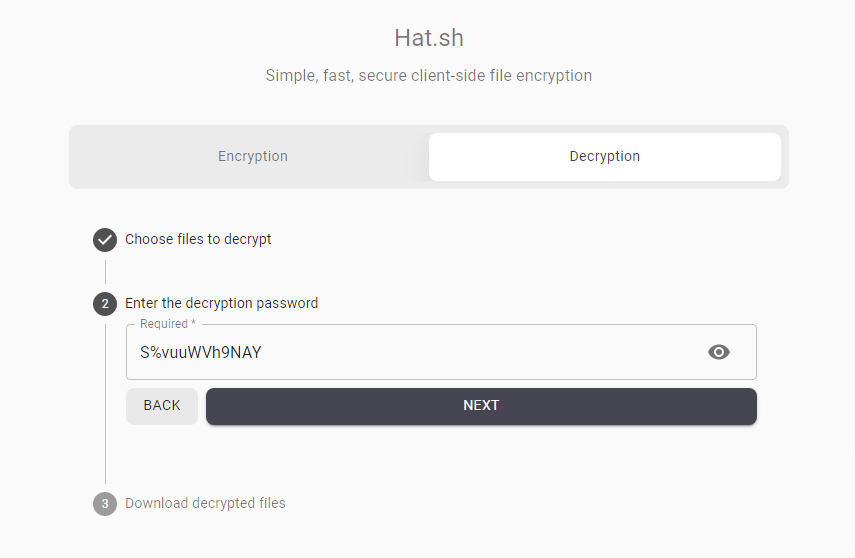




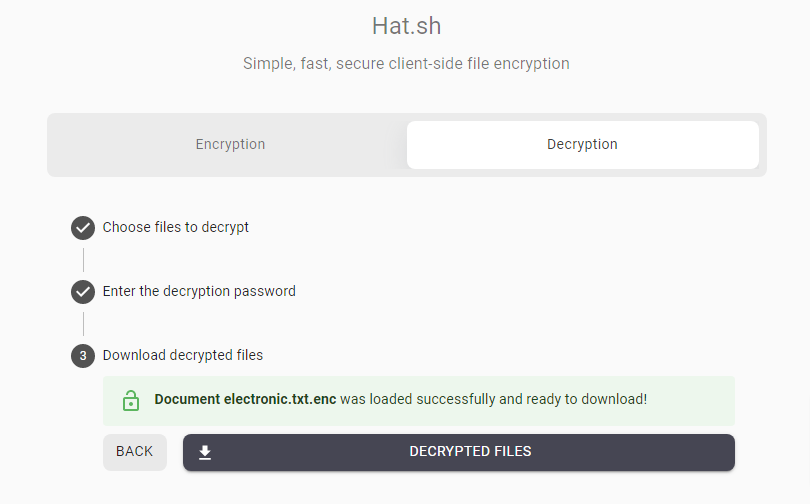
Documentului criptat i s-a schimbat **extensia** initiala, reprezentand faptul ca acea criptare a avut loc.

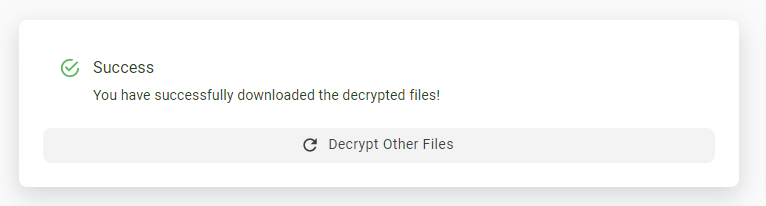


Textul initial este acum **ininteligibil**.

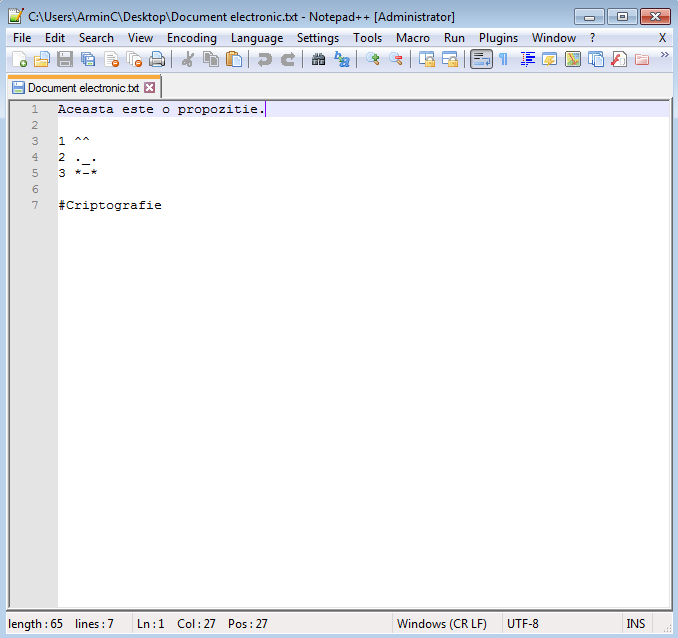


In aceeasi maniera, se va incerca de aceasta data, **decriptarea fisierului**. Se introduce parola stabilita anterior, **S%vuuWVh9NAY**.





Fisierul **decriptat** a fost salvat.



Acesta si-a pastrat in cele din urma **integritatea intiala**.

# Concluzii

Documentele electronice sunt omniprezente in societatea moderna, iar protejarea lor impotriva pierderii, furtului sau a altor amenintari este o preocupare importanta. In acest scop, exista o serie de masuri si tehnici de securitate care pot fi aplicate, atat in ceea ce priveste aspectele tehnologice, cat si politici si proceduri organizatorice.

Una dintre cele mai importante masuri de securitate pentru documentele electronice este criptarea, care poate fi utilizata pentru a proteja datele impotriva accesului neautorizat. De asemenea, autentificarea si autorizarea pot fi utilizate pentru a se asigura ca doar persoanele autorizate au acces la documente importante.

Firewall-urile si antivirusii sunt alte instrumente importante pentru protejarea documentelor electronice impotriva virusilor si altor amenintari de securitate. Backup-ul regulat si recuperarea datelor este de asemenea important pentru a asigura ca documentele electronice pot fi recuperate in caz de pierdere sau deteriorare a datelor.

De asemenea, blocarea documentelor sau restrictionarea acestora cu parola poate fi o masura suplimentara de securitate pentru documentele electronice. Aceasta poate impiedica accesul neautorizat la documente importante si poate asigura ca doar persoanele autorizate au acces la acestea.

Semnaturile digitale pot fi utilizate pentru a verifica autenticitatea si integritatea documentelor electronice si pot fi folosite pentru a asigura ca documentele nu au fost modificate sau falsificate. Semnaturile digitale pot fi utilizate in special pentru documentele care trebuie sa fie semnate si transmise electronic, cum ar fi contracte sau alte documente legale.

Protejarea datelor personale si a confidentialitatii este o alta preocupare importanta in ceea ce priveste documentele electronice. Aceasta ar trebui sa includa masuri de securitate care sa impiedice accesul neautorizat la informatii cu caracter personal si alte date sensibile.

In plus, este important sa se dezvolte politici si proceduri de securitate care sa sprijine utilizarea sigura si responsabila a documentelor electronice. Aceste politici ar trebui sa includa politici de parola puternice, politici de acces si politici de stocare si arhivare a documentelor electronice.

In general, pentru a proteja documentele electronice, este important sa se ia in considerare atat aspectele tehnologice, cat si aspectele organizatorice si sa se dezvolte o abordare integrata a securitatii informatiei. Aceasta poate ajuta la protejarea documentelor electronice impotriva pierderii, furtului sau a altor amenintari de securitate, precum si la protejarea datelor personale si a confidentialitatii in cadrul lor.

# Bibliografie

|  |  |
| --- | --- |
| [1] | "Computer Science," 2023. [Online]. Available: https://www.britannica.com/science/computer-science. |
| [2] | Kodingtech, „Securitatea Informatiilor: De Ce Este Atat De Importanta?,” 2022. [Interactiv]. Available: https://www.kodingtech.com/securitatea-informatiilor-importanta/. |
| [3] | „Criptografie,” 2022. [Interactiv]. Available: https://ro.wikipedia.org/wiki/Criptografie. |
| [4] | J. Fruhlinger, „What is cryptography? How algorithms keep information secret and safe,” 2022. [Interactiv]. Available: https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html. |
| [5] | „Document electronic,” 2018. [Interactiv]. Available: https://ro.wikipedia.org/wiki/Document\_electronic. |
| [6] | Zipper, „5 Beneficii ale arhivarii electronice a documentelor,” [Interactiv]. Available: https://ezipper.ro/media/noutati/5-beneficii-ale-arhivarii-electronice-a-documentelor. |
| [7] | Computer Hope, „Unauthorized access,” 2020. [Interactiv]. Available: https://www.computerhope.com/jargon/u/unauacce.htm. |
| [8] | Malwarebytes, „Computer Virus,” [Interactiv]. Available: https://www.malwarebytes.com/computer-virus. |
| [9] | Microsoft, „Ce este un atac cibernetic?,” 20. [Interactiv]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack. |
| [10] | Bitdefender, „Ce este un atac Man-in-the-Middle (MiTM)?,” [Interactiv]. Available: https://www.bitdefender.ro/consumer/support/answer/79586/. |
| [11] | DespreTot, „Identificarea, autentificarea şi autorizarea accesului,” [Interactiv]. Available: https://despretot.info/identificarea-autentificarea-si-autorizarea-accesului/. |
| [12] | B. K. Jena, „What Is AES Encryption and How Does It Work?,” 2023. [Interactiv]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. |
| [13] | K. AHMAD, „What Is AES-256 Encryption? How Does It Work?,” 2022. [Interactiv]. Available: https://www.makeuseof.com/what-is-aes-256-encryption-how-does-it-work/. |
| [14] | Kiteworks, „Everything You Need to Know About AES-256 Encryption,” [Interactiv]. Available: https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/. |
| [15] | f5, „What is SSL/TLS Encryption?,” [Interactiv]. Available: https://www.f5.com/glossary/ssl-tls-encryption. |
| [16] | Internet Society, „TLS Basics,” [Interactiv]. Available: https://www.internetsociety.org/deploy360/tls/basics/. |
| [17] | appviewx, „What is TLS/SSL Protocol?,” [Interactiv]. Available: https://www.appviewx.com/education-center/what-is-tls-ssl-protocol/. |
| [18] | Cisco, „What Is a VPN? - Virtual Private Network,” [Interactiv]. Available: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html. |
| [19] | Computer Hope, „Backup,” 2023. [Interactiv]. Available: https://www.computerhope.com/jargon/b/backup.htm. |
| [20] | B. Posey, „backup,” 2021. [Interactiv]. Available: https://www.techtarget.com/searchdatabackup/definition/backup. |
| [21] | D. Nield, „How to Password Protect Any File,” 2022. [Interactiv]. Available: https://www.wired.com/story/how-to-password-protect-any-file/. |
| [22] | Locklizard, „Why you should not password protect a Word document,” [Interactiv]. Available: https://www.locklizard.com/document-security-blog/how-to-password-protect-a-word-document/. |
| [23] | Locklizard, „How to Password Protect a PDF File with Adobe & why it is Not Secure,” [Interactiv]. Available: https://www.locklizard.com/how-to-password-protect-pdf-files/. |
| [24] | Uniunea Europeana, „Protecția datelor în conformitate cu RGPD,” 2022. [Interactiv]. Available: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\_ro.htm. |
| [25] | Adobe, „What’s a digital signature?,” [Interactiv]. Available: https://www.adobe.com/sign/digital-signatures.html. |
| [26] | Entrust, [Interactiv]. Available: https://www.entrust.com/resources/faq/digital-signature-vs-electronic-signature. |
| [27] | DocuSign, „Understanding digital signatures,” [Interactiv]. Available: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq. |
| [28] | JASHKOTHARI1, „Cryptography and its Types,” 2023. [Interactiv]. Available: https://www.geeksforgeeks.org/cryptography-and-its-types/. |
| [29] | B. K. Jena, „What Is AES Encryption and How Does It Work?,” 2023. [Interactiv]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption. |