Criptografia – criptarea și decriptarea datelor

Pănescu Vasile-Cosmin

Facultatea de Administrație și Afaceri

Specializarea Cibernetică Economică

Grupa 103

Bazele Tehnologiei Informației

Criptografia – criptarea și decriptarea datelor

Imaginați-vă că trăiți într-o societate în care nu există niciun fel de confidențialitate, în care banii pot dispărea în mod misterios din conturile bancare, în care furtul identității este posibil în orice moment sau în care business-urile pot accesa datele companiilor rivale, iar în final nimeni nu este tras la răspundere. Nimeni nu și-ar dori asta. Din fericire, datorită criptografiei care a evoluat și evoluează în mod constant ca o necesitate a lumii moderne, acest coșmar rămâne doar la stadiul unui exercițiu de imaginație. În aceeași ordine de idei, criptografia constituie procesul de criptare (transformarea unui mesaj dintr-o formă inteligibilă într-o formă greu de înțeles) și decriptare (procesul opus criptării) a mesajelor către/de la expeditor și destinatar, pentru a menține confidențialitatea, integritatea și protecția informațiilor/datelor confidențiale.

Termenul “criptografie” a fost creat prin combinarea termenilor de origine greacă “kryptos”, care înseamnă “ascuns, secret” și “graphein”, care înseamnă “a scrie / scriere”. Astfel, putem defini “criptografia” ca fiind știința codificării unui mesaj într-un format care nu poate fi citit și care este transformat în forma sa originală (inteligibilă) numai de către persoanele potrivite, care sunt capabile să decodifice mesajul respectiv. Această acțiune se realizează folosind o “cheie” secretă, un algoritm de criptare și un algoritm de decriptare (adesea, acești doi algoritmi sunt aceeași).

Pe măsură ce domeniul criptografiei s-a dezvoltat și evoluat, linia delimitatoare dintre ceea ce este și ce nu este criptografia a devenit puțin mai neclară. Criptografia de astăzi poate fi rezumată ca studiul metodelor care se bazează pe existența unor probleme dificile. Majoritatea oamenilor asociază criptarea și decriptarea cu păstrarea confidențialității datelor/comunicațiilor. De fapt, pentru o parte semnificativă a istoriei sale, criptografia a prioritizat protejarea comunicațiilor private. Dar, acesta este doar un aspect al criptografiei moderne.

În continuare, vor fi definite “criptarea” și “decriptarea”, procese indispensabile pentru domeniul criptografiei. Criptarea reprezintă transformarea datelor într-o formă greu/imposibil de înțeles, astfel încât decodificarea lor este aproape imposibilă fără informațiile necesare (de exemplu, o cheie, care poate fi un cuvânt, un număr, o frază, etc.). Rolul acestei acțiuni (de criptare) este de a asigura confidențialitate prin păstrarea informațiilor ascunse de orice persoană căreia nu îi sunt destinate respectivele informații. Pe partea opusă, decriptarea este procesul de conversie a datelor criptate înapoi la forma inițială, adică într-o formă care poate fi înțeleasă/citită; rezumând, decriptarea constituie procesul opus criptării. În cele mai multe cazuri, este necesară o informație secretă, numită cheie, atât pentru criptarea, cât și pentru decriptarea informațiilor. Unii algoritmi folosesc aceeași cheie atât pentru criptare, cât și pentru decriptare. Criptografia din zilele noastre face mai mult decât să cripteze și să decripteze date. Permite de asemenea plățile electronice, protejează companiile de hackeri, etc.. Pe scurt, criptografia “salvează vieți”.

Deși introducerea a venit cu o prezentare a potențialelor efecte dezastruoase date de lipsa criptografiei, o prezentare mai detaliată a beneficiilor și a importanței acesteia este necesară. De asemenea, tratarea acestui subiect este necesară pentru a vedea și a învăța cum datele și identitatea noastră este/trebuie securizată și codificată, astfel încât să avem parte de intimitate și confidențialitate.

Oamenii au folosit, dezvoltat și îmbunătățit comunicarea încă de la începutul timpurilor. De cele mai multe ori, este vital să ne asigurăm că informațiile sunt păstrate în siguranță. Exemplele de lideri, regi și regine din Evul Mediu, generali moderni, etc., arată că intimitatea și confidențialitatea nu pot fi ignorate, în special când vine vorba de sporirea relațiilor. Deci, dorința de intimitate duce la necesitatea creării unor coduri noi și limbaje specifice.

De la email la convorbiri telefonice, de la accesarea securizată a web-ului la banii digitali, criptografia este o parte esențială a sistemelor informaționale de astăzi. Chiar dacă actuala criptografie “de pe piață” nu oferă nivelul de securitate pe care îl promite, corectitudinea, responsabilitatea, acuratețea și mai ales confidentialitatea sunt toate posibile datorită criptarii datelor. Astfel, criptografia poate preveni frauda online și poate garanta legalitatea tranzacțiilor financiare. La fel, poate proteja anonimatul. Poate împiedica hackerii să modifice site-uri web și poate împiedica companiile din a vedea și prelua datele private ale companiei concurente. Criptografia va deveni, de asemenea, din ce în ce mai prioritizata și mai importantă în viitor, pe măsură ce lumea digitală se dezvoltă, iar comunicațiile și afacerile se vor mută în diferite rețele de calculatoare.

Pe de altă parte, prezentarea evoluției criptografiei reprezintă un subiect important, iar tratarea lui este necesară pentru a înțelege mult mai bine această știință, importanța și necesitatea ei, cât și modul în care aceasta a evoluat constant, de-a lungul timpului. În plus, arta de a codifica și decodifica mesaje afectează multe aspecte ale existenței umane, inclusiv politica, economia, societatea și chiar religia. Astfel, dezvoltarea și evoluția criptografiei reprezintă un subiect interesant și necesar pentru discuție.

În criptografie sunt create metode secrete de scriere, cu intenția de a ascunde adevăratul sens al unui mesaj. Acestea se caracterizează printr-un set de obiective și proceduri precise (algoritmi), care au fost dezvoltate pentru prima dată de egipteni, unde mesajul criptat a fost gravat în piatră. Securitatea online este o noțiune frecvent legată de termeni precum “programare”, “codificare” sau “criptografie”, dar legată și de dorința de a dezvolta un sistem unic, în care accesul la date să fie posibil într-un mod sigur, lipsit de riscuri. Criptografia poate fi interpretată drept o practică militară, mai ales atunci când experții britanici au spart codurile cifrului german Enigma, în timpul celui de-al Doilea Război Mondial. Dezvoltarea istorică a criptografiei este sprijinită de contribuțiile lui Caesar, Al-Kindi, Rejewski, Rivest, Shamir, Adleman, etc.. De exemplu, când Iulius Cezar trimitea mesaje generalilor săi, nu avea încredere în mesageri. Astfel, a înlocuit fiecare A din mesajele sale cu un D, fiecare B cu un E și așa mai departe, în tot alfabetul. Numai cineva care cunoștea regula “identarii / schimbării cu 3” (shift by 3) putea descifra mesajele.

Utilizarea computerelor cuantice pentru a rezolva diverse probleme matematice complexe este una dintre cele mai recente inovații în acest domeniu. Când discutăm despre dezvoltarea criptografiei, este importantă concentrarea asupra a trei factori cheie: antic, tehnic și paradoxal.

Cea mai extinsă perioadă de timp este cea antică, întinzându-se din anii 3500 î. Hr. până în secolul al XX-lea, când a fost creată criptografia militară. Egiptenii au inventat hieroglife secrete, care au fost adoptate ulterior în diferite moduri de către multe civilizații a căror limbă era în curs de dezvoltare. În anii 500 î.Hr., limba ebraică a dat naștere cifrului Atbash, o tehnică în care alfabetul era inversat, ceea ce înseamnă că litera A reprezenta litera Z, litera B reprezenta literaY, etc.

Un cunoscut criptograf, Al-Kindi, a propus analiza frecvențelor ca modalitate de a investiga proprietățile literelor prin distribuția lor statistică. Cu timpul, valoarea unor criptări puternice a devenit tot mai clară și evidentă, iar noi concepte au fost adăugate. Cele mai cunoscute au fost cifrul lui Vigenere, care era simplu de înțeles, dar greu de spart, metoda lui Kasiski de criptoanaliză împotriva lui Vigenere și cifrul polialfabetic în formă de placă al lui Alberti. Pentru a-și atinge obiectivele militare, aveau nevoie de coduri noi, iar dezvoltarea de către germani a mașinăriei Enigma a fost una dintre cele mai notabile și importante apariții ale perioadei tehnice (1919 – 1975). Această metodă a fost creată de Arthur Scherbius, care a inclus în mașinărie trei componente cheie: o tastatură pentru introducerea mesajelor text, un codificator pentru criptarea mesajelor și un panou pentru afișarea mesajelor. Însă, deși codul era unul complex (10.000.000.000.000.000 de numere), Rejeswki, un analist polonez, a reușit să îl descifreze. Apoi, ca standard pentru criptografia tehnică, a fost dezvoltată o nouă tehnică de criptare, numită Data Encryption Standard (DES), cu o dimensiune a cheii de 128 de biți (redusă la 56 de biți). Datorită lungimii mari a cheii, algoritmul Triple-DES a înlocuit evoluțiile/realizările recente.

În altă ordine de idei, un cod nou este introdus întotdeauna cu presupunerea că ar putea fi spart. Epoca paradoxală este acum recunoscută ca momentul în care mesajele au fost criptate și decriptate folosind criptarea cu chei publice. Cu o cheie de 4096 de biți, Rivest, Shamir și Adleman au creat unul dintre cei mai recenți algoritmi, RSA (provenit din inițialele numelor lor). Cu toate acestea, chiar și acest cod a fost spart, demonstrându-se dezvoltarea domeniului și stabilind criptografia cuantică ca fiind un domeniu de studiu nelimitat.

După cum a fost deja menționat anterior despre evoluția criptării și decriptării, fiecare secol marchează o nouă realizare cu posibilitatea de a învăța din greșeli (erori) și de a face modificările necesare. Anii 1930 au fost recunoscuți pentru cifrurile militare și nevoia de a le descifra comunicațiile pentru a obține informații necesare. Influența mașinăriei germane Enigma asupra criptografiei în anii 1930 a reprezentat o caracteristică definitorie. Au existat numeroase încercări de a descifra codul, de a înțelege obiectivele și strategiile germane și chiar de a modifica situația respectica. Politica și conflictul de la acel moment au determinat dezvoltarea constantă a criptografiei, însă nu pentru a crea metode noi, inovatoare, ci pentru a le sparge pe cele existente. Însă, decizia japonezilor de a dezvolta o nouă strategie cunoscută sub numele de Purple, a demonstrat că dorința de a câștiga războiul a fost o motivație reală. În toate situațiile, criptarea din anii 1930 nu este altceva decât o tactică militară care accentuează obiectivele liderilor mondiali de la acea vreme. Spre deosebire de anii 1930, anii 1970 au venit cu o multitudine de posibilități și descoperiri care au provocat și inspirat oamenii. Pentru a proteja orice fel de informație, a fost necesară dezvoltarea unui nou sistem de criptare. Cifrul Lucifer era o schemă criptografică sigură, mai simplă decât DES, însă la fel de eficientă. Eforturile de a conecta oamenii prin World Wide Web (WWW) au servit drept fundație pentru criptografia anilor 1970. Cercetătorii și criptografii nu știau nimic despre modul în care internetul ar putea afecta algoritmii și codurile. Ca urmare, au fost efectuate investigații pentru a evalua sistemul și pentru a selecta cele mai bune soluții.

Cele mai complexe metode matematice folosite astăzi în criptografie au fost puse la încercare. Oameni din toate colțurile lumii au dezvoltat deja și încă dezvoltă numeroase moduri de a cripta și decripta datele, perfecționându-și constant expertiza. În comparație cu anii 1930 și 1970, criptografia de astăzi reprezintă o combinație a celor mai bune, dar și celor mai rele descoperiri tehnologice pentru a câștiga putere, a spori confidențialitatea și pentru a promova securitatea în era noastră, era informației.

Trecerea de la cifrurile mecanice la cele digitale marchează o dezvoltare semnificativă în istoria criptografiei. La începutul secoloului al XX-lea, când datele electronice deveneau din ce în ce mai populare și oamenii căutau să își protejeze datele, tehnicile de criptare digitală au câștigat popularitate și au început să fie prioritizate. Tehnicile de criptare digitala diferă de criptarea mecanică prin diverse metode precum: schimbul de date între rețelele telefonice, internetul, tranzacții electronice, televiziune, etc.. Toate aceste schimbări nu au fost ușoare, dar au fost oarecum obligatorii, necesare deoarece lumea și domeniul tehnologiei informației continuă să se schimbe.

Pentru majoritatea mesajelor, calculatoarele reprezintă metoda perfectă de criptare. Capacitatea de criptare a mesajelor astfel încât nimeni să nu le poate citi este într-adevăr interesantă și uimitoare, dar este ceva de care chiar avem nevoie? Probabil multe persoane își pun această întrebare. Mulți dintre noi nu avem nevoie să transmitem mesaje / date criptate, din simplul motiv că nu există persoane interesate de citirea și interceptarea mesajelor / datelor unui om “obișnuit”, “simplu”. Deci, criptarea datelor nu ar fi chiar așa utilă pentru cei care nu au un secret important pe care vor să îl ascundă. Însă, există oameni care trebuie să păstreze secrete importante (persoane care nu sunt neapărat teroriști, criminali, cadre militare, etc.). Spre exemplu, companiile nu ar putea folosi internetul ca mijloc de comunicare dacă acesta ar fi vulnerabil la spionaj. Astfel, pentru business-uri, de exemplu, singura modalitate sigură de a comunica printr-un mediul în care fiecare bit de informație pe care îl trimit poate fi interceptat, este să cripteze toate comunicațiile lor prin diferite metode (cât mai puternice), pentru a rezista împotriva potențialelor și diverselor atacuri.

În final, pentru a încheia tratarea subiectului legat de importanța și necesitatea criptografiei, trebuie precizată una dintre cele mai practice aplicații ale acesteia și anume banii digitali / online. Este o utilitate pe care cu toții o folosim. Fară criptografie ar fi foarte greu să se implementeze o metoda convenabilă pentru existența banilor digitali, bani pe care majoritatea companiilor și persoanelor ar dori să îi aibă.

Din punct de vedere legal, orice informație despre un sistem de criptare puternic este considerată o armă. Asta înseamnă că orice formă de export în altă țară este interzisă. O mișcare “inteligentă” este reprezentată de imigranții ilegali din Franța care și-au tatuat date criptate pe antebrațe, astfel încât să fie ilegal să îi trimită înapoi în țara lor. Întrucât internetul este accesibil tuturor, punerea online a oricărui material care necesită criptare puternică este interzisă. Ceea ce implica faptul că, în prezent, comunicațiile criptate pe internet sunt, de asemenea, ilegale. Totuși, guvernul încearcă să impună Cipul Clipper ca standard pe toate computerele și să interzică toate celelalte forme de criptografie, astfel încât să existe un sistem criptografic unic.

În continuare, următoarea jumătate a referatului se va concentra asupra analizării criptografiei și asupra aspectelor mai tehnice privind criptografia.

Criptografia modernă a avansat până la punctul în care o putem folosi pentru a proteja informații precum numerele cardurilor, voturi, apeluri private, parole, adrese și multe altele. Aș putea continua cu o mulțime de cuvinte despre modul în care criptografia a ajutat și ajută în continuare lumea, însă beneficiile sunt de la sine înțelese pentru toți, depinzând de necesitățile fiecărei persoane.

Cu toate acestea, fiind a doua parte a referatului, voi ilustra cât de uimitoare este criptografia, exemplificând un scenariu care implica Adobe, o companie estimată la aproximativ $150 de miliade, care ar fi putut pierde totul, într-o clipă. În octombrie 2013, Adobe a făcut un anunț, spunând că hackerii au obținut acces la ID-urile, parolele, informațiile și numerele cardurilor la aproape 3 milioane de clienți. Totuși, conform BBC World News: “Numărul de conturi care au fost compromise a fost substanțial mai mare – 38 de milioane!”. În plus, binecunoscutul software de editare, Photoshop, și-a pierdut codul sursă. Când se întâmplă ceva de genul, nu este tocmai o zi bună. Cu toate acestea, în anunțul făcut de Adobe au existat și vești bune. Deși datele au fost preluate de la Adobe, majoritatea dintre ele au fost criptate. Mai exact parolele și numerele cardurilor au fost criptate. Acesta poate reprezenta un atac indirect asupra atacatorilor. Totuși, să ne imaginăm cazul în care datele nu erau criptate. Un adevărat coșmar atât pentru Adobe, cât și pentru milioanele de clienți.

Trecând la un conținut mai tehnic, spunem că știința securității datelor este cunoscută sub numele de criptografie, în timp ce știința analizării și demontării / spargerii comunicațiilor securizate este cunoscută sub numele de criptoanaliză. Procesul de realizare a criptoanalizei presupune un amestec de gândire analitică, utilizarea de instrumente matematice, recunoașterea modelelor, răbdare, tenacitate și chiar un gram de noroc. În aceeași ordine de idei, criptoanaliștii sunt numiți și “atacatori” (motivele fiind evidente și reieșind din definiția criptoanalizei). De asemenea, atât criptografia, cât și criptoanaliza sunt incluse în criptologie.

“Există doua tipuri de criptografie în această lume: criptografia care o va opri pe sora ta mai mică să-ți citească fișierele și criptografia care va împiedica marile guverne să-ți citească fișierele.”

*-Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C*

Evident, criptografia poate fi slabă sau puternică. Puterea criptografică este măsurată în timpul și resursele necesare pentru a recupera textul clar (textul decriptat, sau plaintext). Rezultatul criptografiei puternice este un text criptat (ciphertext) care este foarte greu de descifrat fără posesia unui instrument de descriptare adecvat. Dar cât de dificil ar putea fi? Având în vedere toată puterea de calcul actuală și timpul disponibil, chiar și un miliard de calculatoare care fac un miliard de verificări pe secundă nu ar putea descifra datele criptate ale unei criptografii extrem de puternice, înainte de sfârșitul universului. Un lucru chiar uimitor! Teoretic, criptografia ar trebui să poată rezista chiar și în fața celui mai priceput criptoanalist. Însă nimeni nu a demonstrat că cea mai puternică și bună criptare disponibilă momentan va rezista puterii de calcul a viitorului.

Dar cum funcționează criptografia? Operația matematică utilizată în acest proces de criptare și decriptare a datelor este cunoscută sub numele de algoritm criptografic sau cifru (cipher). Textul clar (plaintext) este criptat folosind o cheie (ex: un cuvânt, un număr, o expresie, etc.) și un algoritm criptografic / cifru. Același text clar poate fi criptat cu mai multe chei pentru a produce text criptat distinct. Puterea metodei criptografice și cheia (privată / secretă) sunt cei doi factori principali care determină cât de sigure sunt datele criptate. Un algoritm criptografic plus toate cheile posibile și toate protocoalele care îl fac să funcționeze formează un criptosistem. În criptografia tradițională, o cheie este utilizată atât pentru criptarea, cât și pentru decriptarea datelor. Aceasta poartă numele de criptare cu cheie secretă (secret-key) sau cheie simetrică. De exemplu, Guvernul SUA utilizează frecvent criptosisteme tradiționale, precum Standardul de Criptare a Datelor (SCD / DES - engleză). Cheile sunt practic numere foarte mari. O cheie de 2048 de biți este un număr întreg foarte mare. Dimensiunea cheii este măsurată în biți, iar securitatea textului criptat crește odată cu dimensiunea cheii.

Când vine vorba de clasificarea criptografiei, există numeroși algoritmi unitizati în criptografie, aceștia împărțindu-se, în general, în trei categorii: criptografie cu cheie publică, criptografie cu cheie privată și criptografie cu funcții hash. Fiecare tip joacă propriul său rol în domeniul criptografic.

Criptografia cu cheie publică este o metodă de criptare în care se folosesc două chei diferite și în care una dintre chei, cea publică, este disponibilă pentru utilizare de către oricine. Cealaltă cheie este cunoscută sub numele de cheie privată. Datele criptate folosind cheia publică pot fi decriptate doar utilizând cheia privată. Datorită utilizării a două chei în loc de una, criptografia cu cheie publică este cunoscută și sub numele de criptografie asimetrică. Acest tip de criptografie este utilizat la scară largă, în special pentru certificatele web TLS/SSL, făcându-se astfel posibil HTTPS (inițial fiind HTTP – care nu oferea caracter sigur website-urilor).

Primul tip de criptare a fost criptarea cu cheie privată, care încă este și cel mai popular tip folosit. Când se utilizează criptografia cu cheie privată, ambele părți trebuie să aibă cheia privata. Totuși, termenul de “cheie” poate fi puțin înșelător, deoarece se referă de fapt la cifrul care este folosit pentru a cripta și decripta datele. Revenind la exemplul cu Cifrul Iulius Caesar, cheia privată era doar un număr care constituia cantitatea cu care fiecare literă din alfabet trebuia identata. Cu toate acestea, în zilele noastre, cheile de criptare sunt reprezentate de algoritmi complexi și extrem de greu, sau chiar imposibil de descifrat. Singurul aspect care rămâne identic pentru criptografia cu cheie privată este că aceeași cheie poate atât cripta, cât și decripta datele. De aceea criptografia cu cheie privată este uneori numită criptografie simetrică.

Algoritmii criptografici cu cheie publică și cheie privată implică transformarea textului clar în text criptat și apoi înapoi în text clar. În schimb, o funcție hash reprezintă un algoritm de criptare unidirecțional, adică odată ce textul clar este criptat, acesta nu poate fi recuperat (decriptat). Poate părea că funcțiile hash sunt inutile, însă factorul cheie este acela că nu există doua texte clare (plaintexts) care să producă același hash (matematic, nu este chiar corect, însă șansele ca acest lucru să se întâmple sunt foarte mici încât pot fi ignorate în siguranță). Acest lucru face ca funcțiile hash să fie o metodă excelentă de asigurare a confidențialității datelor.

În concluzie, nu trebuie niciodată ignorat domeniul criptografiei deoarece reprezintă un aspect inevitabil, necesar și important în lumea modernă. Datorită legăturii sale puternice cu progresul uman și cu cel tehnologic, evoluția croptografiei are una dintre cele mai lungi și mai durabile practici. Criptografia este adaptabilă peste tot, în ciuda faptului că oamenii au folosit întotdeauna informații ascunse, fie pentru a obține un avantaj în luptă, fie pentru a alege cele mai bune strategii militare. Însă aspectele pozitive precum securitatea comunicațiilor și păstrarea sigură a informațiilor personale sunt la fel de semnificative precum capacitatea de a ascunde fapte și de a crea amenințări. Astfel, dezvoltarea criptografiei reprezintă o capacitate umană care trebuie îmbunătățită constant.

Bibliografie:

Bruce Schneier. “Cryptographhy, Security and the Future”. Communications of the ACM. Schneier on Security. Ianuarie 1997. <https://www.schneier.com/essays/archives/1997/01/cryptography_securit.html>.

Simon Singh. “The Code Book”. New York. August 2000.

UKEssays. “An introduction To Cryptology Computer Science”. UKEssays. Noiembrie 2018. <https://www.ukessays.com/essays/computer-science/an-introduction-to-cryptology-computer-science-essay.php>.

Udugahapattuwa. “The fate of cryptography in a post-quantum world”. 2019.

Criptopedia. “Stiinta veche ce va schimba lumea. Totul despre criptografie”. Criptopedia. Noiembrie 2020. [https://www.cryptopedia.ro/educatie/ghid/stiinta-veche-ce-va-schimba-lumea-totul-despre criptografie](https://www.cryptopedia.ro/educatie/ghid/stiinta-veche-ce-va-schimba-lumea-totul-despre%20criptografie).

Aureliu. “Introducere in criptografie”. Aprilie 2018. <https://moodle.usm.md/pluginfile.php/234490/mod_resource/content/0/TEMA%205.%20INTRODUCERE%20%C3%8EN%20CRIPTOGRAFIE.%20Continutul%20temei.pdf>.

Josh Fruhlinger. “What is cryptography? How algorithms keep information secret and safe”. CSO. Mai 2022. <https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html>.