Sveučilište J. J. Strossmayera u Osijeku
Filozofski fakultet Osijek
Preddiplomski studij informatologije

Alojz Šekrst

Kriptografski algoritmi

Završni rad

Mentorica: doc. dr. sc. Anita Papić

Osijek, 2018.

Sveučilište J. J. Strossmayera u Osijeku
Filozofski fakultet Osijek
Odsjek za informacijske znanosti
Preddiplomski studij informatologije

Alojz Šekrst

Kriptografski algoritmi

Završni rad

Područje društvenih znanosti, polje informacijske i komunikacijske znanosti, grana informacijski sustavi i informatologija

Mentorica: doc. dr. sc. Anita Papić

Osijek, 2018.

Sažetak

Razvoj računalnih sustava i rastuća umreženost komunikacijskih kanala koja karakterizira današnje informacijsko doba rezultirali su potrebom za sve temeljitijim sustavima zaštite njihove sigurnosti. Ovaj je rad stoga posvećen kriptografiji čija je zadaća ustanoviti što efikasnije načine šifriranja i dešifriranja. S obzirom na to da jedna osigurava zaštićenost sadržaja poruke od neželjenih osoba, a druga selektivno i ciljano zaprimanje poruke, obje su ove funkcije važne u kriptografskom sustavu. Kriptografski sustav počiva prvenstveno na kriptografskim algoritmima koji sustavno i kontinuirano izvode operacije šifriranja i dešifriranja. Težište samog rada su kriptografski algoritmi opisani kao sekvence operacija koje se koriste za šifriranje i dešifriranje, a koje u osnovi predstavljaju dvije matematičke funkcije. Također, u radu je predstavljena uvriježena podjela kriptografskih algoritama s obzirom na tajnost odnosno javnost ključeva na: simetrične kriptografske algoritme, asimetrične kriptografske algoritme te hibridne kriptografske algoritme. Naime, kod simetričnih kriptografskih algoritama i ključ za šifriranje i ključ za dešifriranje su tajni, a kod asimetričnih kriptografskih algoritama tajan je samo ključ za dešifriranje, dok je ključ za šifriranje javno objavljen. Hibridni kriptosustavi ujedinjuju značajke simetričnih i asimetričnih kriptografskih algoritama. Najpoznatiji simetrični kriptografski algoritmi koji su navedeni u radu su: DES *(Data Encryption Standard) kriptografski algoritam* i AES *(Advanced Encryption Standard) kriptografski algoritam.* Najpoznatiji asimetrični kriptografski algoritam kojemu je u radu posvećena velika pozornost je Rivest-Shamir-Adleman (RSA) kriptografski algoritam. Osim toga, u radu su opisani i neki od najpoznatijih predstavnika hibridnih kriptografskih algoritama kao što su: MD5 *(Message Digest Algorithm)* kriptografski algoritam, SHA-1 *(Secure Hashing Algorithm)* kriptografski algoritam i HMAC *(Hash-based message authentication code)* kriptografski algoritam.

Ključne riječi: kriptografija, kriptografski algoritmi, simetrični kriptosustavi, asimetrični kriptosustavi, hibridni kriptosustavi

Sadržaj

1. Uvod

Kriptografija je kao znanost bitno obilježila razvoj računalne znanosti. Razvoj računalnih sustava i rastuća umreženost komunikacijskih kanala rezultirale su potrebom za sve temeljitijim sustavima zaštite njihove sigurnosti. Zadaća kriptografije je ustanoviti što efikasnije načine šifriranja i dešifriranja. Obje su ove funkcije važne u kriptografskom sustavu jer jedna osigurava zaštićenost sadržaja poruke od neželjenih osoba, dok druga osigurava selektivno i ciljano zaprimanje poruke. Kriptografija, dakle, osigurava sigurnu razmjenu povjerljivih informacija između pošiljatelja i primaoca. Kriptografski sustav počiva najviše na kriptografskim algoritmima koji sustavno i kontinuirano izvode operacije šifriranja i dešifriranja. Do danas su razvijeni brojni kriptografski standardi čije algoritamske funkcije osiguravaju složenu i kvalitetnu kriptografiju sustava u koju je napadačima gotovo nemoguće provaliti.

U drugom poglavlju rada predstavlja se kratki uvod u teoriju algoritama odnosno njihovu definiciju, zadaće algoritama, funkcije algoritama te osnovne vrste algoritama kao i konkretne primjere algoritama. U okviru drugog poglavlja posebno je istaknut Euklidov algoritam kao najstariji algoritam koji je još i danas u upotrebi. Treće poglavlje rada uvodi u kriptografiju dok se četvrto poglavlje rada odnosno središnji dio rada bavi upravo kriptografskim algoritmima kao glavnim osiguravateljima sigurnosti pri komunikaciji, financijskim transakcijama i drugim delikatnim aktivnostima koje se odvijaju putem računalnih sustava. Dakle, u četvrtom poglavlju rada su definirani kriptografski algoritmi, navedene su njihove glavne funkcije, njihove podjele prema različitim kriterijima te su dani prikazi najznačajnijih kriptografskih algoritama. Kriptografski algoritmi se s obzirom na podjelu prema tajnosti, odnosno javnosti ključeva koje koriste dijele na: simetrične kriptografske algoritme i asimetrične kriptografske algoritme. Danas brojni standardi kriptografskih algoritama koriste upravo kombinaciju simetričnih i asimetričnih kriptosustava te se u literaturi nazivaju hibridnima.

Zadaća je ovog rada donijeti pregled problematike vezane uz kriptografske algoritme, predstaviti načine i karakteristike njihove primjene, ukazati na njihovu kompleksnost, sustavnost i funkcionalnost pri izvođenju složenih operacija u kontekstu računalnih sustava te, naposljetku, ukazati na njihovu svrhovitost u osiguravanju postojanja složenih i pouzdanih kriptografskih

sustava. Na kraju se zaključuje kako je kvalitetan kriptografski sustav temelj različitih računalnih sustava koji jamče sigurnost i povjerljivost korisničkih aktivnosti, kako komunikacije s ostalim korisnicima, tako i ovjerenih prijava u sustave, financijskih transakcija te mnogih drugih.

2. Algoritmi

Definicija algoritama je mnogo iako se sve sadržajno poklapaju i priznaju istu zadaću algoritma kao sustavnog načina rješavanja matematičkog problema utvrđivanjem jasnih pravila za dostizanje nekog cilja. Hoško izdvaja definiciju: „algoritam je konačan skup preciznih, razumljivih i jednoznačnih instrukcija koje djelotvorno i učinkovito dovode do rješenja u konačnom vremenu.“[1] Također, pojednostavljeno objašnjava kako je zadaća algoritma matematički problem razbiti na manje cjeline, to jest korake i tako ubrzati njegovo rješenje.[2] Trahtenbrot navodi: „algoritmom se smatra točan propis o izvršenju, određenim redoslijedom, nekog sustava operacija za rješavanje svih operacija nekog zadanog tipa.“[3] Dujella i Marcetić pod algoritmom smatraju „metodu (proceduru) za rješavanje neke klase problema, koja za ulazne podatke određenog tipa daje odgovor (izlazne podatke) u konačnom vremenu.[4]

Ocem algoritma se smatra Abu Ja'far Mohamed ibn Musa al Khowarizmi rođen u Uzbekistanu oko 780. godine. Naziv algoritam nastao je upravo evolucijom njegova imena, Al Khowarizmi, što se s vremenom počelo izgovarati kao algoritam.[5] S pojavom prvih računala u dvadesetom stoljeću pojam algoritma počinje se primjenjivati i na računarstvo.[6] Polazna ideja uporabe algoritama kod računala svodi se na jednostavan princip da računala od trenutka kada su u njih uvedeni polazni podaci (uvjeti zadatka) i program (algoritam za rješavanje) rade bez ikakvog sudjelovanja čovjeka sve do dobivanja konačnog rezultata. Pri tom se procesu odvijaju milijuni aritmetičkih operacija u sekundi.[7]

Kao mali zasebni razrađeni sustavi operacija, algoritmi čine temelje velikih sustava koji pomoću njih samostalno obavljaju najsloženije operacije. Mnogo je značajnih osnovnih algoritama

[1] Hoško, Tomislav. Strukture podataka i algoritmi: priručnik. Zagreb: Algebra, 2009. Str. 9
[2] Isto, str. 8.
[3] Trahtenbrot, Boris Avramovič. Što su algoritmi: algoritmi i računski automati. Zagreb: Školska knjiga, 1978. Str. 13.
[4] Dujella, Andrej. Nav. dj., str. 167.
[5] Usp. Hoško, Tomislav. Nav. dj., str. 8.
[6] Isto, str. 9.
[7] Usp. Trahtenbrot, B. A. Nav. dj., str. 15.

iz teorije brojeva, no sa sigurnošću se kao najvažniji može izdvojiti Euklidov algoritam iz kojeg je izveden i složeniji prošireni Euklidov algoritam.

Euklidov algoritam ili GCD algoritam (Greatest Common Divisor) temelji se na najvećem zajedničkom djelitelju dvaju brojeva; za dva broja a i b najveći zajednički zajednički djelitelj je k. Definicija glasi: GCD (a,b) je najveći broj koji je ujedno djeljiv i s brojem a i s brojem b. Euklid je dao algoritam za sastavljanje GCD-a od dvaju brojeva koji je još i danas nakon nekoliko tisuća godina u upotrebi te je jedan od najvažnijih algoritama u teoriji brojeva.[8] Slijedi razrađeni prikaz Euklidovog algoritma po svim koracima koje algoritam sadrži.

Algoritam 1. Euklidov algoritam[9]

funkcija GCD

ulazni podaci *(input)*

a Pozitivni cijeli broj

b Pozitivni cijeli broj

izlazni podaci *(output)*

k Najveći zajednički djelitelj a i b

postavka

$a \geq 0 \land b \geq 0$

dok je

$a \neq 0$

do

$(a, b) \leftarrow (b \bmod a, a)$

od

povrat

b

Na primjer, tražimo li GCD ili najveći zajednički djelitelj od 21 i 30, izračunat ćemo ga na sljedeći način:

GCD (21,30)

(a,b) = (21,30)

[8] Usp. Ferguson, Niels. Nav. dj., str. 194.
[9] Preuzeto iz: Isto.

U prvom stupnju računamo (30 mod 21) = 9 pa dobivamo (a,b) = (9,21). U sljedećem stupnju računamo (21 mod 9) = 3 pa dobivamo (a, b) = (3,9). Zadnji je stupanj (9 mod 3) = 0 i dobivamo (a,b) = (0,3). Algoritam će dati rezultat 3 koji je zaista i najveći djelitelj 21 i 30.

Suprotnost najvećem zajedničkom djelitelju, GCD-u je LCM (Least Common Multiple) ili najmanji zajednički množitelj. Najmanji zajednički množitelj ili LCM brojeva a i b je najmanji broj koji je ujedno množiv i s brojem a i s brojem b. Primjer: LCM (6,8) = 24. Odnos GCD i LCM moguće je izraziti formulom: LCM (a,b) = ab / GCD (a,b).

Euklidov je algoritam moguće koristiti za pronalaženje cijelih brojeva u i v uz a i b, tako da je GCD (a,b) = va + vb. To bi nam omogućilo izračun a / b (mod p). Ova se verzija Euklidovog algoritma najčešće naziva prošireni Euklidov algoritam.[10]

Algoritam 2. Prošireni Euklidov algoritam[11]

funkcija

Prošireni GCD

ulazni podaci *(input)*

a Pozitivni cijeli broj

b Pozitivni cijeli broj

izlazni podaci (output)

k Najveći zajednički djelitelj a i b

(u,v) Cijeli brojevi tako da va + vb = k

postavka

$a \geq 0 \wedge b \geq 0$

$(c,d) \leftarrow (a,b)$

$(uc, vc, ud, vd) \leftarrow (ud - quc, vd - qvc, uc, vc)$

od

povrat

d (ud, vd)

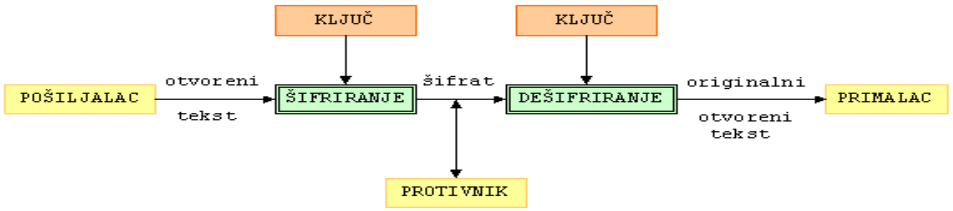
Ovaj algoritam je dosta sličan kao GCD algoritam. Kod njega dodajemo nove varijable c i d umjesto korištenja a i b jer se moramo referirati na originalne a i b u našoj invarijanti.[12]

[10] Usp: Isto, str. 195.
[11] Preuzeto iz: Isto.
[12] Isto.

3. Kriptografija

Kriptografija je, kako ju opisuje Ferguson, umjetnost i znanost enkripcije.[13] Proučava metode slanja poruka u obliku u kojem ih samo onaj kojemu je namijenjena može pročitati. Sama riječ potječe od grčkih riječi kriptós, što znači skriven i gráfo, što znači pisati. Slobodno ju možemo prevesti kao tajnopis.[14] Ona je mali, ali ključan dio sigurnosnog sustava. Kao što je već istaknuto, njena je osnovna zadaća nekim ljudima omogućiti pristup sigurnosnom sustavu te u isto vrijeme nekima zabraniti. Dakle, razlikovati loš pristup od dobrog pristupa. To je puno zahtjevnije od generalne zabrane pristupa sustavu. Upravo zbog toga kriptografija i elementi koji ju okružuju predstavljaju logičnu točku napada na bilo koji sigurnosni sustav. Međutim, ne treba prijevremeno pretpostaviti da je kriptografija slaba točka sustava jer se u praksi pokazalo da rijetko zapravo jest te da je čak i loša kriptografija bolja od ostalih sigurnosnih mjera sustava. Napadači sustava rijetko napadaju kriptografiju; radije pronalaze propuste sustava na drugim mjestima. No, u slučaju da napadač razriješi kriptografiju, male su šanse da bude prepoznat jer neće biti tragova napada, a sustav će napadačev pristup identificirati kao dobar pristup.[15] Kriptiranje ili šifriranje provodi se u nesigurnim komunikacijskim kanalima kao što su telefonska linija ili računalna mreža u kojima je rizično koristiti otvoreni tekst jer postoji opasnost od nadziranja komunikacije od strane takozvanog neprijatelja ili presretača poruke. U tim slučajevima pošiljatelj poruke transformira otvoreni tekst *(eng. plaintext)* koristeći unaprijed dogovoreni ključ *(eng. key)*. Taj se postupak naziva šifriranje, a rezultat je šifrat *(eng. chiphertext)* ili kriptogram. Na taj način presretač može saznati sadržaj šifrata, ali ne i otvoreni tekst koji šifrat zamjenjuje. Za razliku od njega, primalac kojemu je sadržaj šifrata poznat može bez problema dešifrirati poruku.[16] Na Slici 1. vidi se prikaz opisanog modela šifriranja, odnosno dešifriranja.

[13] Ferguson, Niels. Practical cryptography. Indianapolis : Wiley Publishing, 2003. Str. 7.
[14] Usp. Dujella, Andrej ; Maretić, Marcel. Kriptografija. Zagreb: Element, 2007.
[15] Usp. Ferguson, Niels. Nav. dj., str. 8.
[16] Usp. Dujella, Andrej. Nav. dj., str. 1-2.



[17]

Slika 1. Shema klasične kriptografije

Kriptoanaliza ili dekriptiranje bavi se proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.[18] Kriptologija je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.[19]

Moguće je izdvojiti četiri osnovne razine kriptoanalitičkih napada:

1. Samo šifrat - kriptoanalitičar posjeduje samo šifrat, zadatak mu je otkriti otvoreni tekst što više poruka ili ključ kojim su poruke šifrirane;
2. Poznati otvoreni tekst - kriptoanalitičar posjeduje šifrat poruke i njemu odgovarajući otvoreni tekst te mu je zadatak otkriti ključ ili algoritam za dešifriranje;
3. Odabrani otvoreni tekst - kriptoanalitičar može odabrati tekst koji će biti šifriran te dobiti njegov šifrat;
4. Odabrani šifrat - kriptoanalitičar ima pristup alatu za dešifriranje pa može odabrati šifrat i dobiti odgovarajući otvoreni tekst(ovaj je napad tipičan za kriptosustave s javnim ključem);
5. Podkupljivanje, ucjena, krađa i sl. - ne spada izravno u kriptoanalizu, ali se efikasno primjenjuje u kombinaciji s pravim kriptoanalitičkim napadima.[20]

Kako bi borba protiv kriptoanalitičkih napada bila što efikasnija, potrebno je razumjeti algoritme na kojima kriptografski sustav počiva. Upravo su složenost i funkcionalnost algoritama na kojima počiva sustav faktori koji osiguravaju općenitu sigurnost sustava te efikasnu i zaštićenu razmjenu povjerljivih informacija.

[17] Dujella, Andrej. Klasična kriptografija: osnovni pojmovi. URL: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (2014-9-9)
[18] Dujella, Andrej. Nav. dj., str. 2.
[19] Isto.
[20] Usp. Isto, str. 4.

4. Kriptografski algoritmi

Kriptografski algoritmi sekvence su procesa ili pravila kojima se šifriraju ili dešifriraju poruke u kriptografskom sustavu.[21] U osnovi predstavljaju dvije matematičke funkcije koje se koriste za šifriranje i dešifriranje. Njihov je zadatak preslikati elemente otvorenog teksta u elemente šifrata i obratno. Funkcije se biraju iz određenih familija ključeva od kojih je svaka u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva naziva se prostor ključeva. Kriptosustav se sastoji od kriptografskog algoritma, otvorenih tekstova, šifrata i ključeva.[22] Dujella i Maretić tako dolaze do sljedeće formalne definicije: „kriptosustav je uređena petorka (P,C,K,E,D), gdje je P konačan skup svih mogućih osnovnih elemenata otvorenog teksta, C konačan skup svih mogućih osnovnih elemenata šifrata, K konačan skup svih mogućih ključeva, E skup svih funkcija šifriranja i D skup svih funkcija dešifriranja. Za svaki $K \in \mathrm{K}$ postoji funkcija šifriranja $e_K \in \mathrm{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathrm{D}$. Pritom su $e_K : \mathrm{P} \to \mathrm{C}$ i $d_K : \mathrm{C} \to \mathrm{P}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in \mathrm{P}$. "Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$. Iz njega slijedi da funkcije e_K moraju biti injekcije. Zaista, ako bi bilo $e_K(x_1) = e_K(x_2) = y$, za dva različita otvorena teksta x_1 i x_2, onda primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2, tj. $d_K(y)$ ne bi bilo definirano. U skladu s tim imamo da ako je $\mathrm{P} = \mathrm{C}$, onda su funkcije e_K permutacije."[23] Kriptografski algoritmi imaju širok raspon upotrebe, uključujući osiguravanje sigurnih i ovjerenih financijskih transakcija.[24]

Dujella i Marcetić navode također klasifikaciju kriptosustava s obzirom na tri kriterija:

1. Tip operacija koje se koriste pri šifriranju -
   postoji podjela na supstitucijske šifre u kojima se svaki element otvorenog teksta zamjenjuje s nekim drugim elementom i transpozicijske šifre u kojima se elementi otvorenog teksta permutiraju (premještaju);
2. Način na koji se obrađuje otvoreni tekst -
   ovdje postoji podjela na blokovne šifre kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ K te protočne šifre *(engl. stream*

[21] What are cryptographic algorithms? URL: http://www.wisegeek.com/what-are-cryptographic-algorithms.htm (2014-09-05)
[22] Dujella, Andrej; Maretić, Marcel. Nav. dj., str. 2.
[23] Isto.
[24] What are cryptographic algorithms? URL: http://www.wisegeek.com/what-are-cryptographic-algorithms.htm (2014-09-05)

cipher) kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći paralelno generirani tip ključeva *(engl. key stream);*

3. Tajnost i javnost ključeva -
   ovdje je osnovna podjela na simetrične kriptosustave i sustave s javnim ključem. Kod simetričnih ili konvencionalnih kriptosustava sigurnost leži u tajnosti ključa zbog čega se nazivaju i kriptosustavima s tajnim ključevima. Kod kriptosustava s javnim ključem ili asimetričnih kriptosustava ključ za dešifriranje se ne može izračunati iz ključa za šifriranje. Kod takvih sustava bilo tko može koristiti javni ključ za šifriranje, ali za dešifriranje je potrebno imati tajni ili privatni ključ. Ideju o javnom ključu prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine.[25]

U literaturi se uglavnom koristi razlikovna podjela kriptografskih algoritama s obzirom na tajnost, odnosno javnost ključeva, tj. podjela na simetrične, asimetrične te hibridne kriptografske algoritme. Kako je već spomenuto, simetrični kriptografski algoritmi imaju tajni ključ za šifriranje, dok asimetrični imaju javni ključ.

4.1. Simetrični kriptosustavi

Simetrična kriptografija najstariji je tip kriptografije te potječe barem još iz doba starih Egipćana. Takva kriptografija koristi samo jedan ključ ujedno i za šifriranje i dešifriranje, otuda termin simetrična. Zbog sigurnosnih mjera nužno je da tajni ključ nikada ne bude otkriven. Većina simetričnih algoritama kao tehnike šifriranja koristi supstituciju i permutaciju. Što se ove tehnike više puta uzastopno koriste, to je sustav sigurniji. Nelinearnost je također važna za sigurnost sustava. Ona se postiže korištenjem nelinearnih supstitucijskih tablica *(eng. S-boxes)* gdje su izlazni podaci *(eng. output)* manji od ulaznih podataka *(eng. input)* ili pak obrnuto.[26]

Mnoge su prednosti simetrične kriptografije: relativno jeftina proizvodnja snažnih ključeva za šifrate, relativno jeftina obrada algoritama te puno veća razina zaštite od veličine ključa. Zbog toga implementiranje simetrične kriptografije u sustave može biti vrlo učinkovito jer ne dolazi do značajnog kašnjenja rezultata nakon provođenja šifriranja i dešifriranja. Također pruža sigurnost autentifikacije jer podaci koji su šifrirani jednim ključem ne mogu biti dešifrirani ijednim drugim.

[25] Dujella, Andrej; Maretić, Marcel. Nav. dj., str. 3.
[26] Usp. Mukhopadhyay, Sourav. The DES Algorithm. URL: http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf (2014-09-05).

Dok god je simetrični ključ kao tajna zadržan između dva korisnika, komunikacija je sigurna.[27] Međutim, glavni je problem simetrične kriptografije distribucija ključa. Naime, kako bi kriptografija funkcionirala, obje strane moraju imati kopiju tajnog ključa. Pri tome svaka razmjena zahtjeva očuvanje tajnosti ključa, što zahtjeva sigurni komunikacijski kanal koji nije tako lako postići.[28]

Neki od najpoznatijih simetričnih kriptografskih algoritama su DES *(Data Encryption Standard)* i AES *(Advanced Encryption Standard).*

4.1.1. Standard za dešifriranje podataka

Standard za dešifriranje podataka (DES-*Data Encryption Standard)* metoda je koja se koristi za šifriranje, odnosno dešifriranje podataka korištenjem privatnog ili tajnog ključa. Ovom je metodom moguće koristiti 72 kvadrimilijuna ili više mogućih enkripcijskih ključeva. Za svaku se poruku ključ odabire slučajno među ovim velikim brojem mogućih ključeva.[29] DES-ov ključ sastoji se od 64 binarne znamenke (nula ili jedinica), od kojih je 56 bita nasumično generirano i primjenjuje se izravno na algoritam. Ostalih 8 bita koje algoritam ne koristi mogu se koristiti za detektiranje pogrešaka. Proces se može izvoditi na razne načine te uključuje šesnaest krugova operacija. Podaci se mogu vratiti iz šifrata samo korištenjem istog ključa koji je korišten za kodiranje. Neovlašteni primatelji šifrata koji znaju algoritam, ali nemaju ispravan ključ ne mogu algoritamski dobiti originalne podatke. Međutim, može biti izvedivo odrediti ključ koristeći brutalnu silu napada. Također, svatko tko ima ključ i algoritam može lako dešifrirati šifrat i dobiti uvid u originalne podatke.

Standardni algoritam temelji se na sigurnom ključu, čime pruža osnovu za razmjenu šifriranih računalnih podataka izdavanjem ključa korištenog u šifriranju onima koji su ovlašteni imati te podatke.[30] Radi boljeg šifriranja, često se koristi i trostruki DES algoritam. DES je izradio IBM (*International Business Machines)* 1977. godine te je prihvaćen od strane Ministarstva obrane Sjedinjenih Američkih Država. Pod pretpostavkom da ovaj kriptografski algoritam može biti

[27] Symmetric cryptography. URL: http://pic.dhe.ibm.com/infocenter/tpfhelp/current/index.jsp?topic=%2Fcom.ibm.ztpf-ztpfdf.doc_put.cur%2Fgtps7%2Fs7symm.html (2014-09-09).
[28] Mukhopadhyay, S. Nav. dj.
[29] Usp. Search Security: Data Encryption Standard (DES). URL: http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (2014-09-06).
[30] Data Encryption Standard. // Federal Information Processing Standard Publications 46-3, 10 (1999), str. 1-2. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (2014-09-10).

korišten od strane neprijateljskih vlada, američka je vlada zabranila njegov izvoz u druge države. Međutim, besplatna inačica softvera je široko dostupna.[31]

4.1.2. Unaprijeđeni standard za dešifriranje podataka

Unaprijeđeni standard za dešifriranje podataka (*Advanced Encryption Standard)* je, kao što naziv govori, unaprijeđeni DES koji se koristi za zaštitu povjerljivih podataka američke vlade. Inicijativu za pronalaženjem snažnijeg kriptografskog algoritma od DES-a pokrenuo je *National Institute of Standards and Technology (NIST),* jedinica Ministarstva trgovine Sjedinjenih američkih država. Algoritam koristi blok za dešifriranje veličine 128 bita koji podržavaju ključeve veličine 128, 192 i 256 bita. Od algoritma se zahtijevalo da bude oslobođen od naknade za korištenje širom svijeta i ponudi sigurnost na dovoljnoj razini za zaštitu podataka naredih 20 do 30 godina. Također, polazna ideja bila je i mogućnost lakog provođenja u hardver i softver, kao i u ograničene sredine kao što su npr. pametne kartice. Za ovaj je standard NIST pokrenuo proces selekcije najpogodnijeg algoritma koji je bio otvoren javnoj raspravi. U uži je izbor ušlo pet algoritama: MARS, RC 6, Rijndael, Serpent i Twofish. Implementacije svih algoritama bile su testirane u jezicima ANSI C i Java na brzinu i pouzdanost u brzini šifriranja i dešifriranja te otpornosti ključeva i algoritama na razne napade. Nakon provedenih testiranja NIST je objavio da je Rijndael odabran kao predloženi standard. Godine 2001. Ministarstvo trgovine službeno je odobrilo *Federal Information Processing Standard (FIPS)* 197 koji određuje da će svi povjerljivi dokumenti koristiti Rijndael kao *Advanced Encryption Standard.*[32]

4.2. Asimetrični kriptosustavi

Asimetrična kriptografija ili kriptografija javnog ključa kriptografija je u kojoj se koristi par ključeva za šifriranje i dešifriranje kako bi poruka sigurno stigla. U početku mrežni korisnik prima javni i tajni ključ od ovlaštene osobe. Svaki drugi korisnik koji želi slati šifriranu poruku može doznati javni ključ primaoca iz javnog direktorija. Taj korisnik pomoću javnog ključa šifrira

[31] Usp. Search Security: Data Encryption Standard (DES). URL: http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (2014-09-06)
[32] Usp. Search Security: Advanced Encryption Standard (AES). URL: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard (2014-09-06).

poruku te ju šalje primatelju. Kada primatelj dobije poruku, dešifrira ju pomoću privatnog ključa kojemu nitko drugi nema pristup.[33]

Prvi su asimetričnu kriptografiju javno predložili Witfield Diffie i Martin Hellman, istraživači na Sveučilištu Stanford u svom radu New Directions in Cryptography 1977. godine. Sam koncept je nekoliko godina prije predložio James Ellis nekoliko godina ranije dok je radio u sjedištu za komunikacije britanske vlade. Diffie i Hellman navode u svom radu brojne prednosti asimetričnog kriptosustava. Kao prvo, zahtjeva razmjenu samo jednog ključa. Druga je prednost da kvaliteta kriptografije eksponencijalno raste s uloženim trudom korisnika. Treća prednost je to što se njezina upotreba može vezati uz javni dokument ili korisničke informacije koje služe potvrdi autentičnosti korisnika A korisniku B i obrnuto. Opisuju asimetrični algoritam kao *„trap door"*, „vrata-zamka", što bi značilo da je to jednosmjerna funkcija koju je lako izvesti u jednom smjeru, no teško ju je ili gotovo nemoguće preokrenuti.[34] Na primjer, lako je izračunati rezultat od dva broja, ali je računski mnogo teže naći dva faktora koji daju samo njihov rezultat. Ako imamo ponuđene ujedno i rezultat i jedan od faktora, lako je izračunati drugi faktor, što ukazuje na činjenicu da je težak smjer računanja moguće olakšati kada se pruži pristup tajnom ključu. Funkcija koja se koristi i ključ opće su poznati, no te informacije ne omogućuju dešifriranje poruke. Jedina informacija koja je potrebna i dovoljna za dešifriranje poruke je tajni ključ primatelja.[35] Uz kriptosustave s javnim ključem veže se i ideja digitalnog potpisa poruke koju su 1967. godine opisali Diffie i Hellman. Digitalni potpis omogućuje prenošenje korisnih svojstava „potpisa na papiru" u digitalno okruženje te autentifikaciju (moguće je provjeriti je li poruka poslana ciljanom primatelju) i nepobitnost (pošiljatelj poruke ne može poreći da je poruku poslao jer primatelj posjeduje poruku s potpisom pošiljatelja).[36]

Jedan od najkorištenijih i najpoznatijih asimetričnih algoritama je RSA (Rivest-Shamir-Adleman) algoritam.

[33] Usp. Search Security: Asymetric cryptography (public-key cryptography). URL: http://searchsecurity.techtarget.com/definition/asymmetric-cryptography (2014-09-06).
[34] Diffie, Whitfield; Helmann, Martin E. New directions in cryptography: Invited paper. URL: http://courses.isi.jhu.edu/netsec/papers/new_directions.pdf (2014-09-08). Str. 34., 37.
[35] Usp. Usp. Search Security: Asymetric cryptography (public-key cryptography). Nav. dj.
[36] Usp. Dujella, A. Nav. dj, str. 155.

4.2.1. Rivest-Shamir-Adleman (RSA) algoritam

Algoritam su 1977. godine izumili Ronald Rivest, Adi Shamir i Leonard M. Adleman. Prvi put ga je javnosti iste godine predstavio Martin Gardner u časopisu *Scientific American*. Zasnovan je na problemu faktorizacije, što znači da teškoća faktorizacije velikih prirodnih brojeva jamči sigurnost. U samom se šifriranju i dešifriranju, međutim, koristi modularno potenciranje, dok se faktorizacija koristi u dobivanju dodatnog podatka *(„trapdoora")*.[37] Ključ koji se koristi za dešifriranje drukčiji je od ključa koji se koristi za dešifriranje. Ta su dva ključa međusobno povezana. Algoritam se temelji na množenju dvaju prirodnih brojeva i dodatnih operacija iz kojih proizlazi skup dvaju brojeva koji čini javni ključ te drugi skup koji čini privatni ključ. Nakon što se razviju ključevi, izvorni prirodni brojevi nisu više važni i mogu biti odbačeni. I javni i privatni ključevi važni su za šifriranje, ali samo vlasnik privatnog ključa ga treba znati. Koristeći RSA sustav, privatni ključ se nikada ne treba slati putem interneta. Privatni se ključ koristi za dešifriranje teksta koji je kodiran javnim ključem. Dakle, kad pošiljatelj pošalje poruku, može saznati javni ključ primaoca od centralnog administratora i šifrirati poruku za njega. Pošiljatelj, međutim, ne može saznati privatni ključ primaoca. Dobivenu poruku od pošiljatelja primatelj dešifrira pomoću svog privatnog ključa.[38] Ovaj se algoritam na opisani način može izravno iskoristiti za ostvarivanje digitalnog potpisa.

4.3. Hibridni kriptosustavi

Hibridni kriptosustavi su oni koji, kako sam naziv govori, ujedinjuju više vrsta kriptosustava. Kombinacije simetričnih i asimetričnih kriptosustava izrađuju se radi iskorištavanja prednosti obje vrste kriptosustava. Te se prednosti ogledaju u brzini i sigurnosti. Shema hibridne kriptografije spaja praktičnost sheme asimetričnog šifriranja i učinkovitost sheme asimetričnog šifriranja. Hibridna kriptografija postiže se prijenosom podataka koristeći jedinstvene sesije ključeva zajedno sa simetričnim šifriranjem. Javni ključ za šifriranje implementiran je za slučajna šifriranja pomoću simetrične kriptografije. Primatelj tada koristi metodu šifriranja pomoću javnog ključa kako bi dešifrirao simetrični ključ. Nakon što se simetrični ključ otkrije, moguće ga je koristiti za dešifriranje poruke. Kombiniranje metoda dešifriranja ima razne prednosti. Jedna od

[37] Usp. Dujella, A. Nav. dj., str. 102.
[38] Usp. Search Security: RSA algorithm (Rivest-Shamir-Adleman). URL: http://searchsecurity.techtarget.com/definition/RSA (2014-09-06).

njih je uspostava kanala koji povezuje set opreme dvaju korisnika. Korisnici imaju mogućnost komunicirati kroz hibridno dešifriranje. Asimetrično šifriranje može usporiti proces dešifriranja, ali uz istodobno korištenje simetričnog šifriranja, poboljšavaju se oba oblika dešifriranja. Rezultat je dodana sigurnost procesu prosljeđivanja zajedno s općim unaprjeđenjem performansi sustava.[39]

Neki od najpoznatijih algoritama koji kombiniraju značajke simetričnih i asimetričnih algoritama su MD5 algoritam *(Message Digest Algorithm),* SHA-1 *algoritam (Secure Hashing Algorithm)* i HMAC algoritam *(Hash-based message authentication code).* Svi su ovi algoritmi kreirani za autentifikaciju digitalnog potpisa poruke, mehanizma koji se prvotno vezao uz asimetrične kriptografske sustave. Za spomenute algoritme karakteristično je korištenje tzv. *hash* funkcija. *Hash* funkcija je odobrena matematička funkcija koja preslikava niz proizvoljne duljine na niz fiksne duljine.[40] *Hash* funkcije se u računarstvu koriste za različite primjene kao što su brzo uspoređivanje, identifikacija ili brzo pretraživanje.[41]

4.3.1. MD5 *(Message Digest)* algoritam

MD5 algoritam koristi se za potvrdu autentičnosti podataka kroz stvaranje poruke od 128 bita stvorene od ulaznih podataka. Ta je poruka jedinstvena i kompatibilna sa skupom podataka kao što je slučaj s pojedincem i otiskom prsta. MD5 razvio je profesor Ronald L. Rivest na MIT-u (*Massachusetts Institute of Technology*) za upotrebu aplikacija za digitalni potpis, što iziskuje da se velike datoteke kompresiraju sigurnom metodom prije dešifriranja pomoću tajnog ključa, pod kriptosustavom javnog ključa. MD5 treća je generacija algoritma za provođenje poruka koji je kreirao Rivest. Prethodne verzije su MD2 i MD4. Sve tri verzije imaju slične strukture, s tom razlikom što je MD2 optimiziran strojeve od 8 bita, a ostale dvije za strojeve od 32 bita. MD5 algoritam proširenje je MD4 algoritma. Kritičkim osvrtom ustanovljeno je da je MD4 brz, no možda nije dovoljno siguran. U usporedbi s njim, MD5 nije toliko brz, ali nudi bolje osiguranje sigurnosti podataka.[42] MD5 algoritam implementiran je u brojne programske jezike uključujući C, Perl i Javu.

[39] Techopedia: Hybrid Encryption. URL: http://www.techopedia.com/definition/1779/hybrid-encryption (2014-09-09).
[40] The Keyed-Hash Message Authentication Code. // Federal Information Processing Standards Publications 198, 3 (2002), str. 10. URL: http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf (2014-09-09).
[41] Dujella, A. Nav. dj., str. 143.
[42] Usp. SearchSecurity: MD5. URL: http://searchsecurity.techtarget.com/definition/MD5 (2014-09-09).

4.3.2. SHA-1 *(Secure Hashing Algorithm)* algoritam

SHA-1 *(Secure Hashing Algorithm)* algoritam dizajnirala je Agencija za nacionalnu sigurnost Sjedinjenih Američkih država (United States National Security Agency). Objavio ga je NIST 1995. godine. SHA-1 izbacuje 160 bita datoteka ili ulaznih podataka bilo koje veličine. U konstrukciji je sličan *hash* funkcijama MD4 i MD5, ali je jači. Koristi veličinu bloka od 521 bita i ima maksimalnu veličinu poruke od 2^{64} - 1 bita.[43] Koristi se kako bi osigurao integritet podataka; predstavlja garanciju da podaci nisu bili izmijenjeni tijekom prijenosa te za autentifikaciju; garantira da je podatak došao iz izvora iz kojeg je trebao doći. SHA-1 je proizveden kako bi se koristio zajedno sa standardom za digitalni potpis. Stručnjaci iz područja kriptologije uočili su malobrojne slabosti SHA-1 pa je zato nastala poboljšana verzija, SHA-2. Međutim, SHA-1 se pokazao kao siguran algoritam čije hakiranje do sada nije evidentirano.[44]

4.3.3. MAC *(The Message Authentication Code) algoritam*

MAC *(The Message Authentication Code)* tehnika je za izvođenje autentifikacije poruka koja se široko koristi. MAC algoritmi uključuju korištenje tajnog ključa za generiranje malog bloka podataka pridruženog poruci, poznatog kao kod za autentifikaciju poruke. Ova tehnika pretpostavlja da dvije stranke koje komuniciraju dijele tajni ključ. Kad pošiljatelj šalje poruku primaocu, on izračunava kod autentičnosti poruke koji je u funkciji poruke i ključa. Poruka i kod prenose se ciljanom primatelju. Primatelj izvodi isti izračun na primljenoj poruci koristeći isti tajni ključ za generiranje novog koda za autentifikaciju poruke. Primljeni kod uspoređuje se s izračunatim kodom. Ako se oni ne razlikuju, znači da poruka nije presretena od strane napadača. Ovaj je proces sličan dešifriranju s tom razlikom što algoriram za identifikaciju ne mora biti reverzibilan kao što je slučaj kod dešifriranja. Zbog matematičkih karakteristika funkcije za autentifikaciju, manje je izgledno da će biti provaljen, za razliku od algoritama šifriranja.[45]

[43] SHA1 Description. URL: http://www.cs.rit.edu/~bcw5910/482/TeamFlux.pdf (2014-09-09).
[44] Usp. Internet-Computer-Security.com: MD5 i Sha-1 algorithm – VPN Tutorial. URL: http://www.internet-computer-security.com/VPN-Guide/Sha-1.html (2014-09-09).
[45] Usp. Dr.Dobb's: The HMAC Algorithm. URL: http://www.drdobbs.com/security/the-hmac-algorithm/184410908 (2014-09-09).

4.3.4. HMAC *(keyed-Hashing for Message Authentication)* algoritam

HMAC *(keyed-Hashing for Message Autentication)* varijacija je MAC-a koja je postala standard brojnih aplikacija. HMACje autentifikacijski kod poruke koji koristi kriptografski ključ u kombinaciji s *hash* funkcijom.[46] Ciljevi HMAC-a su: bez modifikacija koristiti dostupne *hash* funkcije, omogućiti jednostavne zamjene ugrađenih *hash* funkcija u slučaju da su otkrivene ili potrebne brže ili sigurnije *hash* funkcije, očuvati izvornu izvedbu *hash* funkcije bez značajne degradacije, koristiti i rukovati ključevima na jednostavan način te imati kriptografsku analizu snage mehanizama autentifikacije bazirane na razumnim pretpostavkama o ugrađenim *hash* funkcijama.[47] Bilo koja kriptogfrafska *hash* funkcija, kao što su MD-5 i SHA-1 mogu se koristiti za izračun u HMAC-u. Kriptografska snaga HMAC-a ovisi o kriptografskoj snazi temeljnih *hash* funkcija. Veličina izlaznih podataka HMAC-a jednaka je kao i veličina temeljne *hash* funkcije te iznosi 128 ili 160 bita u slučaju MD5 ili SHA-1, iako može biti smanjena po želji. Definiciju i analizu konstrukcije HMAC-a prvi su put objavili Mihir Bellare, Ran Canetti i Hugo Krawczyk 1996. godine.

[46] The Keyed-Hash Message Authentication Code. Nav. dj., str. 10.
[47] Isto.

5. Zaključak

Kriptografski algoritmi imaju u kriptografskom sustavu ključnu operativnu ulogu pri ostvarivanju kriptografskih ciljeva šifriranja ili dešifriranja. Najčešće je zadatak kriptografskih algoritama osigurati sigurnost prijenosa podataka i potvrdu autentičnosti korisnika. Znanstvenici iz područja kriptografije kontinuirano i sustavno donose algoritamske standarde te ih unaprjeđuju kreirajući nove inačice. Sve to upućuje na činjenicu kako je jedna od glavnih preokupacija računalne znanosti danas zaštita povjerljivih podataka te osiguravanje nesmetanog prijenosa podataka sigurnim komunikacijskim kanalima do ciljanog primatelja. Simetrični algoritmi ili algoritmi s tajnim privatnim ključem jednostavni su za korištenje u kriptografiji upravo zbog svoje simetričnosti koja se ogleda u tajnosti oba ključa. Velika slabost takvih algoritama koju treba uzeti u obzir je problem distribucije ključa, što je kod asimetričnih algoritama riješeno na način da je pošiljatelju poruke poznat ključ za šifriranje. Javni ključ olakšava slanje šifrirane poruke do primatelja koji ju, budući da ima na raspolaganju tajni privatni ključ, lako može dešifrirati. Najbolja kvaliteta kriptografskih sustava postiže se kombiniranjem značajki simetričnih i asimetričnih algoritama. Tako nastaju složeni kripto-sustavi koje je teže hakirati. Svi opisani kripto-sustavi izuzetno su sigurni, iako svaki ima slabosti. Unaprjeđenjem kvalitete i složenosti kripto-sustava poboljšava se cjelokupna kriptografija. Kriptografija je ključna za svaki računalni sustav jer ujedno i omogućuje pristup koji detektira kao dobar te sprječava loš pristup. Bitno je poduzeti sve mjere zaštite kriptografije upravo iz razloga što se nakon provaljivanja u kriptografiju napadaču ne može ući u trag, a ponekad ni primijetiti da je napad počinjen. Ako želimo osigurati sigurnost računalnih sustava, moramo poznavati algoritme na kojima ti sustavi počivaju.

Literatura:

1. Accuhash: What is MD5?. URL: http://www.accuhash.com/what-is-md5.html (2018-09-09).

2. Data Encryption Standard. // Federal Information Processing Standard Publications 46-3, 10 (1999), str. 1-2. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (2018-09-10).

3. Diffie, Whitfield; Helmann, Martin E. New directions in cryptography: Invited paper. URL: http://courses.isi.jhu.edu/netsec/papers/new_directions.pdf (2018-09-08).

4. Dr.Dobb's: The HMAC Algorithm. URL: http://www.drdobbs.com/security/the-hmac-algorithm/184410908 (2014-09-09).

5. Dujella, Andrej ; Maretić, Marcel. Kriptografija. Zagreb: Element, 2007.

6. Dujella, Andrej. Klasična kriptografija: osnovni pojmovi. URL:https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html (2018-9-9)

7. Ferguson, Niels. Practical cryptography. Indianapolis : Wiley Publishing, 2003.

8. Hoško, Tomislav. Strukture podataka i algoritmi: priručnik. Zagreb: Algebra, 2009.

9. Internet-Computer-Security.com: MD5 i Sha-1 algorithm – VPN Tutorial. URL: http://www.internet-computer-security.com/VPN-Guide/Sha-1.html (2018-09-09).

10. Mukhopadhyay, Sourav. The DES Algorithm. URL: http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf (2018-09-05).

11. Search Security: Advanced Encryption Standard (AES). URL: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard (2018-09-06).

12. Search Security: Asymetric cryptography (public-key cryptography). URL: http://searchsecurity.techtarget.com/definition/asymmetric-cryptography (2018-09-06).

13. Search Security: Data Encryption Standard (DES). URL: http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (2018-09-06).

14. Search Security: RSA algorithm (Rivest-Shamir-Adleman). URL: http://searchsecurity.techtarget.com/definition/RSA (2018-09-06).

15. SearchSecurity: MD5. URL: http://searchsecurity.techtarget.com/definition/MD5 (2018-09-09).

16. Techopedia: Hybrid Encryption. URL: http://www.techopedia.com/definition/1779/hybrid-encryption (2018-09-09).

17. The Keyed-Hash Message Authentication Code. // Federal Information Processing Standards Publications 198, 3 (2002). URL: http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf (2018-09-09).

18. Trahtenbrot, Boris Avramovič. Što su algoritmi: algoritmi i računski automati. Zagreb: Školska knjiga, 1978.

19. What are cryptographic algorithms? URL: http://www.wisegeek.com/what-are-cryptographic-algorithms.htm (2018-09-05).