CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Metode zaštite dokumenata

NCERT-PUBDOC-2010-04-296

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Zaštita osjetljivih dokumenata je gorući problem u današnjem svijetu. Porastom broja krađa podataka u digitalnom obliku (USB uređaji, prijenosna računala i dr.), zaštita podataka na računalu i vanjskim uređajima za pohranu podataka postala je prioritet za mnoge tvrtke koje u svakodnevnom poslovanju koriste povjerljive i osjetljive podatke. Iako danas postoje brojna besplatna i komercijalna rješenja za zaštitu podataka na računalima i drugim medijima za pohranu, mnoge tvrtke još uvijek nisu upoznate s mogućnostima i prednostima koje ona nude, kao niti s rizicima koje donosi potencijalna krađa povjerljivih informacija. Curenje krivih informacija u krivo vrijeme može imati drastične financijske posljedice za neku tvrtku, u ekstremnim situacijama čak i kobne po poslovanje. Stoga se većina organizacija pokušava zaštiti od neovlaštenog pristupa osjetljivim dokumentima.

Danas postoji sve veća potreba za zaštitom osjetljivih informacija. U povijesti su ljudi koristili različite metode kojima su pokušavali osigurati tajnost i integritet važnih podataka. Mnoge od tih metoda uključivale su jednostavne algoritme (npr. prikaz jednog znaka drugim) koji su vrlo brzo razbijeni. Razvojem matematičkih znanosti, tehnologije i računarstva, došlo je do pojave profinjenih algoritama koji su sadržavali složene matematičke proračune. Kriptiranje, ograničavanje pristupa i zaštita dokumenata iza vatrozida (eng. *firewall*) neke su od uobičajenih tehnika zaštite osjetljivih informacija. Uz takve metode koristi se i digitalno potpisivanje dokumenata i digitalni vodeni žigovi.

U dokumentu su navedeni razlozi upotrebe zaštite dokumenata, zatim su opisane metode zaštite dokumenata, kao i algoritmi zaštite koji se primjenjuju za komprimirane datoteke. Također, dan je primjer zaštite cijelog diska. U posljednjem poglavlju opisane su mogućnosti razbijanja zaštite dokumenata.

2. Zašto štititi dokumente?

Dokumenti su temeljni poslovni resurs svake organizacije jer sadrže ključne informacije o poslovanju, kao što su planovi, izvještaji, poslovni rezultati, projekti, nacrti, izračuni, sheme i slično. Veliki broj dokumenata predstavlja neku vrstu intelektualnog vlasništva i poslovnu tajnu te zahtijeva najveću moguću razinu nadzora i zaštite pristupu dokumentu, kao i raspolaganja njegovim sadržajem. Zaštita dokumenata postaje teško ostvariv zadatak uz trend zamjene papirnatih dokumenata elektroničkim oblikom. Digitalne dokumente važno je zaštititi od neovlaštenog kopiranja i upotrebe, kao i od curenja podataka osjetljivih dokumenata te prijetnji povjerljivosti i integritetu podataka u dokumentu. Gubitak dokumenata zbog slučajnog brisanja, prepisivanja, kvarenja čvrstog diska može stajati tvrtku mnogo novaca i uzrokovati gubitak produktivnosti. U današnjem poslovnom okruženju očekuje se da je moguće zaštititi dokumente od neovlaštenog pristupa, iskorištavanja ranjivosti alata za čitanje dokumenata te od neprimjerene upotrebe .

Organizacije koje posjeduju dokumente s važnim i povjerljivim informacijama, posebnu pažnju poklanjaju sljedećim aspektima sigurnosti:

- **tajnost**– podaci u dokument smiju biti pristupačni samo ovlaštenim korisnicima,
- **autentičnost** – jednoznačno prepoznavanje ovlaštenih korisnika,
- **odgovornost** - praćenje pristupa i izmjena,
- **integritet** - upozorenje je li dokument bio mijenjan i
- **izvornost** - provjera izvora dokumenta.

Oduvijek je postojala potreba zaštite osjetljivih podataka, a time i dokumenata koji sadrže takve podatke. Tokom povijesti razvijeno je mnogo metoda kojima su ljudi pokušavali i uspijevali očuvati tajnost važnih podataka. Mnoge metode su bile jednostavne i nisu pružale dovoljnu zaštitu. U takvim slučajevima tajnost je često bila narušena. Razvojem kriptografije i tehnologije otkriveni su vrlo dobri načini kriptiranja i zaštite dokumenata. Kriptiranje je dobar način sprječavanja neovlaštene osobe od pregledavanja sadržaja osjetljivog dokumenta. Ali kada se dokument dekriptira tajnim ključem, ovlaštena osoba loših namjera može spremiti, kopirati, ispisati ili proslijediti dokument. Ograničavanje pristupa dokumentu nekolicini pojedinaca jedan je od pristupa zaštite dokumenta, no uvijek postoji mogućnost da jedna od osoba kojoj je povjeren pristup oda podatke. U tom slučaju treba se pronaći osobu koja je odala informacije, što nije uvijek jednostavan zadatak. Rješenje koje osigurava zaštitu osjetljivih informacija ne može ovisiti o samo jednoj tehnologiji. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite.

3. Algoritmi zaštite dokumenata i njihova sigurnost

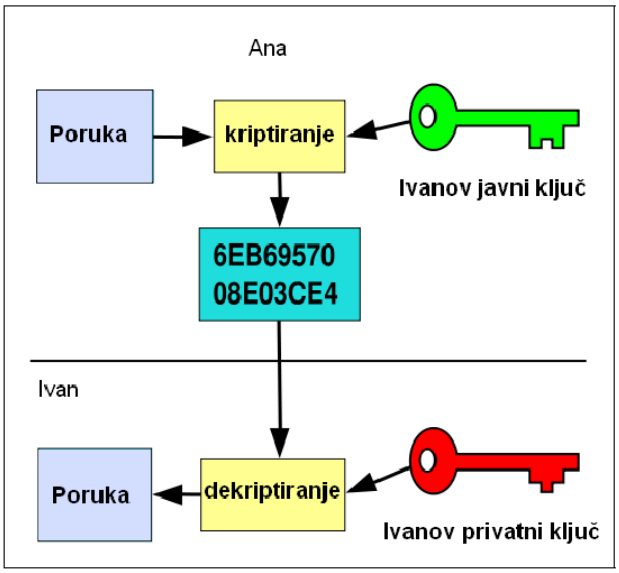
Postoji mnogo metoda zaštite dokumenata. Neke od značajnijih su: kriptiranje, upotreba digitalnih vodenih žigova, lozinki, kriptografskih sažetaka te digitalnih potpisa.

3.1. Kriptiranje

Važan dio zaštite dokumenata pohranjenih na tvrdim diskovima računala, posebno prijenosnih, svakako je enkripcija. Ovim relativno jednostavnim postupkom moguće je izbjeći otkrivanje povjerljivih informacija u slučaju gubitka prijenosnog računala, kao i napade zlonamjernih korisnika koji ostvare fizički pristup računalu. Većina modernih operacijskih sustava posjeduje ugrađene mehanizme koji omogućuju kriptiranje pohranjenih podataka.

Postupak kriptiranja uključuje preoblikovanje otvorenog ili jasnog teksta u tekst nerazumljiv osobama kojima nije namijenjen. Osobe kojima je dokument namijenjen i koje ga smiju pročitati moraju posjedovati poseban ključ za pretvaranje dokumenta u jasan tekst, odnosno dekriptiranje. Postoje simetrični i asimetrični kriptosustavi. U simetričnom kriptosustavu ključ kriptiranja ili pretvaranja dokumenta u nerazumljiv tekst jednak je ključu dekriptiranja, dok kod asimetričnog kriptosustava to nije slučaj. U komunikaciji porukama obično postoji pošiljatelj i primatelj poruke. Neka je poruka dokument sa osjetljivim podacima koji se razmjenjuje. Ukoliko se koristi simetrični kriptosustav za dekriptiranje, primatelj treba poznavati ključ kojim je dokument kriptiran. Ključ posjeduje samo osoba koja je kriptirala dokument i primatelj jedino od nje može dobiti ključ. Prema tome, potrebno je obaviti razmjenu ključeva, odnosno pošiljatelj treba na neki način poslati ili osobno predati ključ kojim primatelj može dekriptirati dokument. Takav se ključ naziva tajnim ključem i koristi se za kriptiranje i dekriptiranje poruke, što znači da primatelj može dekriptirati dokument samo upotrebom istog ključa kojim je kriptirana. Kako bi došao do tog ključa pošiljatelj mu mora na neki način predati ključ, odnosno primatelj i pošiljatelj moraju obaviti razmjenu tajnog ključa. Najčešće korišten protokol za razmjenu tajnog ključa je Diffie-Hellmanov protokol [12].

Asimetrični kriptosustavi zasnivaju se na određenim svojstvima brojeva koja se istražuju u teoriji brojeva. Ideju objašnjava sljedeći primjer. Ana stvara samo svoj par ključeva: jedan za kriptiranje i jedan za dekriptiranje. Ako se pretpostavi da je asimetrično kriptiranje oblik računalne enkripcije, tada je Anin ključ za kriptiranje jedan broj, a ključ za dekriptiranje neki drugi broj. Ana svoj dekripcijski ključ drži u tajnosti te se on zbog toga obično naziva privatnim ključem. Ona, međutim, svoj ključ za kriptiranje javno objavljuje tako da je on svakome dostupan. Zbog toga se obično on naziva javni ključ. Ako Ivan želi Ani poslati poruku, jednostavno će potražiti njezin javni ključ, koji će biti objavljen u nečemu sličnom telefonskom imeniku. Zatim će Ivan njezinim javnim ključem kriptirati poruku i poslati je. Kada poruka stigne, Ana ju može dekriptirati svojim privatnim ključem. Na isti način bilo tko može Ani poslati kriptiranu poruku. Velika prednost sustava je što on uklanja problem distribucije ključa. Poruku može dekriptirati samo Ana jer jedino ona posjeduje privatni ključ.



Slika 1. Upotreba asimetričnog kriptosustava. Izvor: CARNet CERT

Primjer najčešće korištenog asimetričnog kriptosustava je RSA, čiji su autori Ron Rivest, Adi Shamir i Len Adleman. Još neki primjeri takvih algoritama su ElGamal, NTRUEncrypt, LUC i drugi.

Sigurnost kriptiranih dokumenata ovisi o tome koji se algoritam koristi za kriptiranje te duljini kriptografskih ključeva. Napadači mogu provesti kriptoanalizu teksta kojeg žele dekriptirati. Kriptoanaliza je znanstvena disciplina koja proučava metode otkrivanja značenja kriptiranih informacija bez pristupa tajnim informacijama za dekriptiranje. Obično se takve metode zasnivaju na poznavanju rada sustava te pronalaženju tajnog ključa. Izraz kriptoanaliza ponekad se odnosi na pokušaj zaobilaženja sigurnosti kriptografskih algoritama ili protokola, a ne samo kriptografske zaštite. Ipak, kriptoanaliza obično uključuje metode napada koje ne ciljaju na ranjivosti poput socijalnog inženjeringa ili krađe i zapisivanja lozinki unesenih preko tipkovnice. Kriptoanaliza se može provesti nagađanjem ključa (ovisno o tome koliko se informacija može otkriti) ili korištenjem informacija o sustavu koji se napada. Kao osnovna točka početka kriptoanalize obično se uzima pretpostavka kako je neprijatelju sustav poznat (Kerckhoffov princip). Ovo je razumna pretpostavka u praksi jer postoje brojni „tajni" algoritmi koji su probijeni kroz povijest.

Osnovne vrste kriptoanalize uključuju:

- **samo kriptirani tekst** (eng. *ciphertext-only*) - napadač ima pristup samo skupini kriptiranih tekstova.
- **poznati izvorni tekst** (eng. *known-plaintext*) – napadač ima skupinu kriptiranih tekstova za koje poznaje odgovarajući nekriptirani tekst.
- **izabrani (ne)kriptirani tekst** (eng. *chosen-plaintext/ciphertext*) – napadač može otkriti (ne)kriptirani tekst koji odgovara skupini (ne)kriptiranog teksta po njegovom vlastitom odabiru.
- **prilagodljivi izabrani nekriptirani** tekst (eng. *adaptive chosen-plaintext*) – poput prethodnog, osim što napadač može izabrati sljedeći nekriptirani tekst na temelju informacija koje je prikupio u prethodno opisanom načinu dekriptiranja.
- **napad odgovarajućim ključem** (eng. *related-key attack*) – poput izabranog (ne)kriptiranog teksta, osim što napadač može otkriti kriptirani tekst kriptiran s dva različita ključa. Pri tome, ključevi nisu poznati napadaču, ali poznat je odnos među njima (npr. kakva je razlika).

Zbog ostvarenja što bolje sigurnosti korisnici trebaju paziti pri odabiru veličine kriptografskog ključa.

Kod upotrebe asimetričnog kriptosustava napadaču je jednostavnije izvesti napad na javni nego na privatni ključ. To znači da je potrebno odabrati veličinu javnog ključa koji sadrži više bitova od privatnog ključa. Uz to, privatni ključ bi trebao biti dva puta „bitovno duži" (sadržavati najmanje dvostruko više bitova) od ključa koji se razmjenjuje. Treba imati na umu da 1024 bitni prosti broj koji se koristi pri stvaranju javnog ključa ima efektivnu dužinu od 160 bitova u privatnom ključu. To znači da, ako privatni ključ treba biti 2 puta duži od tajnog ključa, moguće je sigurno razmijeniti ključ duljine 80 bitova. Napad grubom silom na takav ključ zahtjeva računanje 80^2 mogućnosti. Na dovoljno dobrom računalu takav ključ se može izračunati za sat vremena. Prema tome ovisno o potrebnoj razini zaštite komunikacije

potrebno je odabrati prosti broj za računanje javnog ključa i privatni ključ veće dužine (na primjer prosti broj dužine 2048 bitova).

3.2. Zaporke

Zaporka je oblik tajnog podatka kojeg je potrebno poznavati da bi se pristupilo određenim resursima, informacijama i slično. Zaporka se čuva od onih koji danim resursima ne smiju imati pristup, dok se oni koji pokušavaju resursima pristupiti provjeravaju znaju li lozinku ili ne (prema čemu im se dozvoljava ili odbija pristup). To je kombinacija znakova (slova, simbola, brojeva i tako dalje) koje računalo pamti (ili pamti kako prepoznati zaporku). Svaki put kad korisnik želi pristupiti podatku pod zaporkom od njega se traži upisivanje iste, čuvajući time njegovu privatnost. Dokumenti se, dakle, mogu zaštititi i dodavanjem zaporke. Na taj se način ograničava pristup dokumentu.

Zaporka treba biti takva da ju je lako zapamtiti, a teško pogoditi. Međutim takve su zaporke obično nesigurne jer ljudi ne pamte lako različite kombinacije nizova znakova koje uključuju mala i velika slova, brojeve i posebne znakove.

Sigurnost dokumenata zaštićenih zaporkom ovisi o nekoliko faktora. Računalo na kojem se nalazi dokument mora imati antivirusni program. Način pohrane zaporki na računalu je također važan faktor. Na nekim računalima zaporke se pohranjuju u obliku čistog teksta. To nije siguran način pohrane zaporki jer ju bilo koji korisnik računala može pročitati. Sigurnija metoda pohrane je upotreba kriptografskih sažetaka. Umjesto pohrane zaporki, pohranjuju se kriptografski sažeci zaporki. Kada korisnik upisuje zaporku, njezina autentičnost se provjerava usporedbom kriptografskog sažetka upisane zaporke i pohranjene zaporke. Često se kod pohrane sažetaka zaporki dodaje još jedna vrijednost kako bi se spriječilo napadače da stvore svoju listu sažetaka često korištenih zaporki.

3.2.1. Sigurnost zaporki

Napadač uvijek može pokušati razbiti zaporku. Pojam „razbijanje zaporki“ obično je ograničen na otkrivanje jedne ili više zaporki pomoću kojih se dobiva poznata vrijednost sažetka. Postoje mnogi načini dobivanja zaporki, zbog čega napadač može i bez sažetka pokušati pristupiti na računalni sustav (npr. pogađanjem same zaporke). Jedan od sustava zaštite je dobar dizajn sustava koji ograničava broj pokušaja neuspješnog pristupa i obavještava administratora (kako bi takav sustav, ako je potrebno, privremeno isključio). Ipak, poduzimanje velikih mjera zaštite ponekad nije dovoljno da bi se sustav obranio od napada.

Napadač može koristiti različite metode za otkrivanje zaporki, a neke od njih su:

- **pogađanje zaporki**,
- **napad grubom silom** (eng. *brute force*) - isprobavanje svake moguće zaporke,
- ***dictionary* napad** - isprobavanju zaporka iz prethodno pripremljenih rječnika,
- **prebrojavanje** – stvaranje sažetka svakog niza znakova u rječniku,
- **tehnike socijalnog inženjeringa** (eng. *social engineering*) - problem korištenja raznih komunikacijskih vještina u uvjeravanju korisnika da postupe na određeni način,
- **praćenje telefonskih i Internet veza** bez znanja sudionika komunikacije,
- **prikriveno snimanje unosa na tipkovnici** (eng. *keystroke logging*),
- ***login spoofing*** - korisnik upisuje korisničko ime i zaporku u posebno oblikovan program te tako napadaču otkriva osjetljive informacije,
- ***dumpster diving*** - pronalaženje korisnih informacija filtriranjem materijala koje je korisnik odbacio u smeće (najčešće *post-it* poruke s korisničkim imenima i zaporkama),
- ***phishing*** - usmjeravanje korisnika na unos detalja na web stranicama putem poruka elektroničke pošte ili izravnom razmjenom poruka (primjer je prikazan na slici 2),
- ***shoulder surfing*** - dobivanje informacija izravnim motrenjem („gledanje preko ramena“),
- ***timing attack*** - ugrožavanje sustava analizom vremena potrebnog za izvođenje kriptografskog algoritma,
- **trojanski konj ili virus** - korištenje zlonamjernog programa da bi se zavarao korisnik (program korisniku ne izgleda zlonamjerno) i
- **kompromitiranje sigurnosti poslužitelja**.

3.3. Digitalno potpisivanje dokumenata

Kao potpis rukom, digitalni potpis jedinstveno pripada osobi koja ga je stvorila. Za razliku od tradicionalnih potpisa, digitalni potpisi mogu sadržavati dodatne informacije, poput datuma i vremena potpisa ili razloga potpisa.

Digitalnim potpisom (eng. digital signature - DS) se utvrđuje autentičnost elektroničkih dokumenata, kao što su elektroničko pismo, web stranica ili slika. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da njegov integritet nije narušen. Vjerodostojnost (eng. authentication) potpisanih dokumenata provjerava se upotrebom kriptografskih metoda. Postupak digitalnog potpisivanja dokumenta sastoji se od:

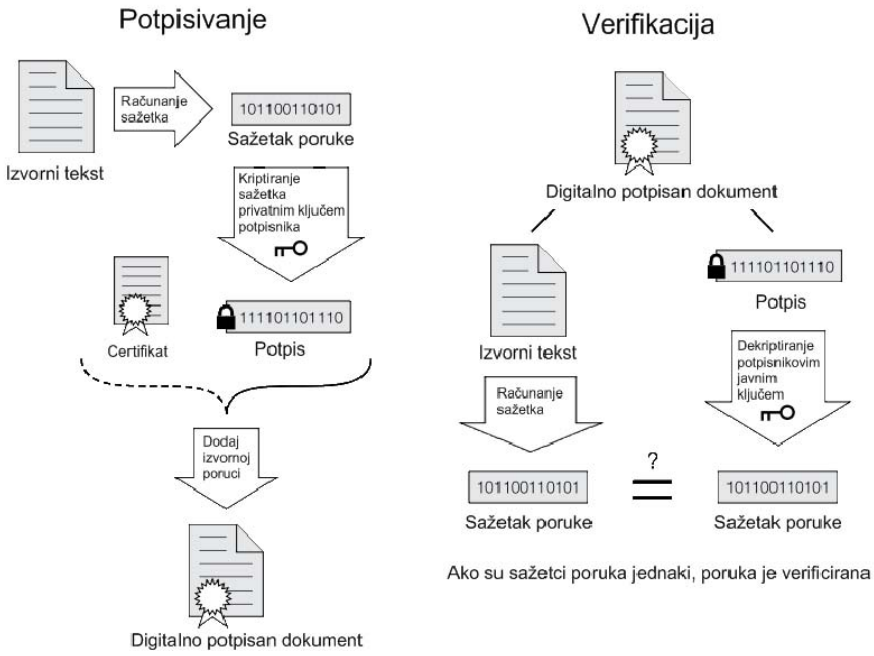
- izračunavanja sažetka poruke (izvornog teksta) – na primjer MD5 algoritmom i
- kriptiranja sažetka poruke.

Digitalni potpis osigurava:

- autentičnost - identitet pošiljatelja utvrđuje se dekriptiranjem sažetka poruke,
- integritet ili besprijekornost poruke - utvrđuje se je li poruka izmijenjena na putu do primatelja
- neporecivost - pošiljatelj ne može poreći sudjelovanje u transakciji jer jedino on ima pristup do svog privatnog ključa kojim je potpisao poruku

U stvaranju digitalnog potpisa, odnosno u postupku kriptiranja sažetka poruke koristi se asimetrični kriptografski postupak. Kriptografski saželi (eng. *hash, cryptographic digest*) u širokoj su upotrebi u današnje vrijeme. Za izračunavanje sažetka poruke koriste se posebne funkcije (eng. *hash functions*). Te funkcije stvaraju svojevrsni digitalni otisak određene veličine. Spomenuti je otisak zapravo niz znakova koji se obično zapisuju u heksadekadskoj notaciji. Dobre funkcije za izračunavanje sažetaka za različite ulazne podatke daju različite sažetke, odnosno dobiveni sažetak je jedinstven za svaku pojedinu poruku. Digitalni potpisnik stvara par ključeva, privatni i javni. Privatnim ključem kriptira sažetak poruke te tako stvoreni digitalni potpis šalje ili objavljuje zajedno s potpisanom porukom. Osnova sigurnosti digitalnog potpisa je u tajnosti privatnog ključa dok je javni ključ svima dostupan. Najčešći algoritam koji se koristi za kriptiranje sažetka poruke je RSA.

Sljedeći primjer prikazuje digitalno potpisivanje dokumenta.



Slika 2. Digitalno potpisivanje dokumenta
Izvor: CARNet CERT

Neka Ana i Matko razmjenjuju poruke. Ana želi osigurati autentičnost, besprijekornost i neporecivost poruke. Kako bi to postigla ona digitalno potpisuje poruku. Pri tome koristi svoj privatni ključ za

kriptiranje sažetka poruke izračunatog, na primjer, MD5 algoritmom (privatni ključ inače služi za dekriptiranje!). Ana šalje poruku:

$$M = (P, RSA(H(P), K_{DA})$$

gdje je P izvorna poruka (razgovijetni tekst), RSA algoritam kriptiranja, *H(P)* je sažetak poruke (izračunat korištenjem npr. MD5 algoritma) i K_{DA} je Anin privatni ključ.

Dakle, Ana je kriptirala sažetak poruke svojim privatnim ključem i u poruku koju šalje Matku uključila izvornu poruku i kriptirani sažetak te poruke.

Matko Aninim javnim ključem (koji inače služi za kriptiranje!) obavi dekriptiranje:

$$H(P) = RSA^{-1}(RSA(H(P), K_{DA}), K_{EA}),$$

gdje je H(P) sažetak poruke, RSA^{-1} postupak dekriptiranja, K_{DA} Anin privatni ključ, K_{EA} Anin javni ključ i $RSA(H(P), K_{DA})$ sažetak poruke kriptiran RSA algoritmom upotrebom Aninog privatnog ključa.

Matko je dekriptiranjem sažetka Anine poruke saznao dvije činjenice:

- da je poruku uistinu poslala Ana, jer samo ona i nitko drugi ne poznaje njezin privatni ključ
- da je pristigla poruka P besprijekorna

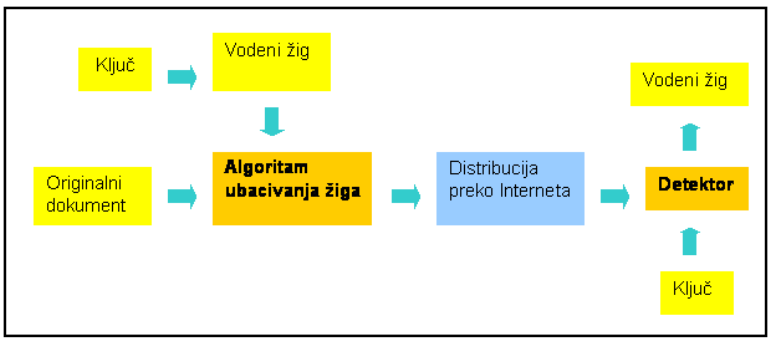
Kriptirani sažetak čini svojevrsni potpis, tj. digitalni potpis koji je Ana poslala uz poruku. Detaljniji oblik ovog digitalnog potpisa ovisi o sadržaju poruke.On je za svaku poruku drugačiji.

3.4. Digitalni vodeni žig

Efikasna sigurnost ostvaruje se svim prethodno spomenutima tehnologijama s time da mora ostaviti otisak na samom dokumentu. Pod ostavljanjem otisaka smatra se ugrađivanje jedinstvene informacije u dokument, koja identificira vlasnika ili primatelja dokumenta. Ugrađena informacija može se detektirati i dekodirati u bilo kojem trenutku, čak i nakon ispisa i skeniranja. Proces ostavljanja otisaka u dokumentu može se postići uporabom tehnika označavanja digitalnim vodenim žigom.

Označavanje digitalnim vodenim žigom je tehnika kojom se mogu zaštiti autorska prava različitih multimedijskih sadržaja. S obzirom da postoji više različitih multimedijskih formata kao što su slike, audio podaci, video podaci te grafički objekti, potrebno je razviti posebne metode za svaki od njih. U usporedbi s istraživanjima o označavanju slika, video i audio podataka, istraživanja o označavanju teksta su malobrojna. Ipak pojavom novih primjena kao što su npr. digitalna knjižnica te knjige u elektroničkom formatu raste interes i za ovo područje.

Osnovna ideja označavanja digitalnim vodenim žigom je stvaranje meta podataka koji sadrže informacije o digitalnom mediju koji se želi zaštititi. Meta podaci su vodeni žig koji se može neprimjetno ugraditi u željeni medij. Vodeni žig treba biti otporan na namjerna i nenamjerna izobličenja.



Slika 3. Ubacivanje digitalnog vodenog žiga.

Sustav za označavanje digitalnim vodenim žigom sastoji se od dva glavna dijela:

- podsustav za ugrađivanje vodenog žiga i
- podsustav za detekciju.

Ugrađivanje kombinira dokument, odnosno audio vizualni signal u koji se ugrađuje informacija, i poruku (eng. *payload*), koja se dodaje dokumentu, čime se stvara označeni sadržaj. Algoritam označavanja ima dva koraka. U prvom se koraku poruka kodira u vodeni žig koji mora biti istog tipa i istih dimenzija kao i dokument. Ako je, npr., dokument slika, tada i vodeni žig mora biti uzorak slike istih dimenzija kao i izvorna slika. Bolja sigurnost može se postići korištenjem ključa vodenog žiga u procesu kodiranja. U drugoj fazi, vodeni se žig dodaje dokumentu kako bi se stvorio označeni dokument.

Slika 4. Primjer slike sa vodenim žigom
Izvor: Developing Webs.net

Postoje dvije vrste označavanja:

- slijepo i
- informirano.

Vrsta označavanja ovisi o tome koristi li se dokument prilikom stvaranja vodenog žiga ili ne. Za slijepo označavanje nije potreban izvoran dokument. Vodeni žig se dobiva kodiranjem dokumenta uz pomoć ključa vodenog žiga. Informirano označavanje koristi informacije iz izvornog dokumenta prije stvaranja vodenog žiga. Detektori, odnosno dekoderi vodenih žigova također se dijele na dvije vrste - slijepe i informirane. Vrsta označavanja ovisi o tome koliko informacija o dokumentu je dostupno prilikom procesa detektiranja vodenog žiga. Informirani detektor koristi izvorni dokument u procesu detekcije.

3.4.1. Lomljivi vodeni žigovi

Lomljivi se žigovi zovu tako jer je poželjno da se prilikom primjene većine tehnika obrade dokumenata izmjene ili unište. Svojstva lomljivog žiga su:

- nevidljiv je promatraču,
- mijenja se prilikom primjene većina tehnika za obradu dokumenata,
- neovlaštene osobe ne bi smjele moći ubaciti lažni vodeni žig,
- ovlaštene osobe mogu brzo izvaditi vodeni žig,
- očitani vodeni žig pokazuje gdje je došlo do promjena.

3.4.2. Otporni vodeni žigovi

Ova vrsta vodenih žigova se zove „otporni žigovi“ jer se očekuje da budu postojani neovisno o napadima. Svojstva otpornog žiga su:

- nevidljiv je promatraču,
- ostaje u dokumentu čak i nakon obrade dokumenta,
- neovlaštene osobe teško mogu detektirati vodeni žig,
- ovlaštene osobe mogu brzo izvaditi vodeni žig,

- nakon što je dokument ispisan i skeniran i dalje je moguće učitati vodeni žig.

Stvaranje algoritama koji posjeduju svojstva da neovlaštene osobe teško mogu detektirati vodeni žig i da je nakon ispisa i skeniranja dokumenta i dalje moguće učitati vodeni žig težak je zadatak, ali otporan vodeni žig nije pretjerano koristan ako se može lagano ukloniti. Također, teško je razviti programski sustav koji će detektirati vodeni žig čak i nakon većine izmjena. Za ostvarivanje svojstva da neovlaštene osobe teško mogu detektirati vodeni žig preporuča se korištenje vodenih žigova koji zahtijevaju poseban ključ za učitavanje.

4. Metode zaštite Office dokumenata

4.1. Microsoft Office dokumenti

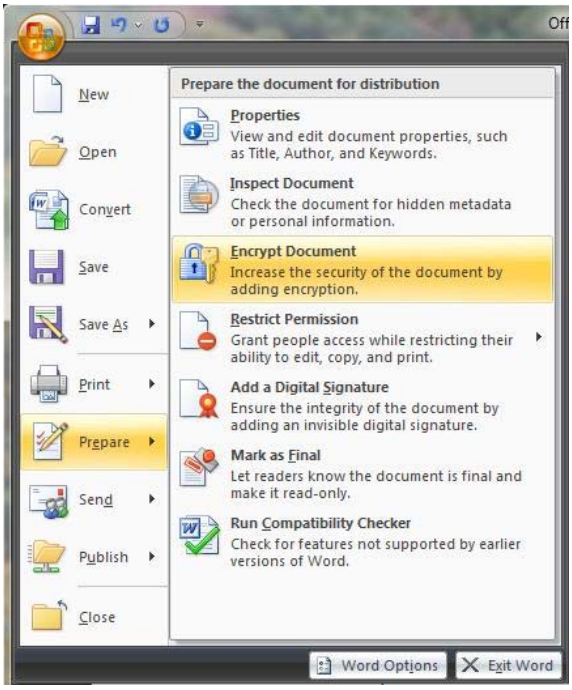
Paket Microsoft Office 2007 nudi nekoliko metoda zaštite dokumenata, uključujući enkripciju, postavljanje sigurnosnih ograničenja na uređivanje i formatiranje te upotrebu digitalnih potpisa.

Zaštita dokumenata zaporkom postoji već dugo vremena u Office sustavima. Sustavi prije Office 2007 su koristili algoritam kriptiranja RC4 s duljinom ključa 128 bitova. Metoda enkripcije koja se koristila upotrebljavala je isti inicijalizacijski vektor za kriptiranje različitih inačica istog dokumenta, što znači da se koristio isti ključ za kriptiranje. Takav način kriptiranja predstavljao je ranjivost jer su napadači mogli uspoređivati kriptirane dokumente kako bi otkrili sadržaj i neovlašteno pročitali podatke dokumenta. Microsoft Office 2007 koristi AES algoritam za kriptiranje koji je mnogo bolji od RC4. Pretpostavljena duljina ključa kod kriptiranja AES algoritmom je 128 bitova, no može se povećati na 256 bitova. Uz to koristi SHA-1 algoritam stvaranja kriptografskih sažetaka. Svojstva kriptiranja dokumenata u programskom paketu Microsoft Office 2007 su:

- upotrebom Microsoft Office 2007 moguće je kriptirati samo Word 2007 dokumente, Excel 2007 dokumente i PowerPoint 2007 prezentacije,
- pretpostavljeni algoritam enkripcije je 128 bitni AES. Moguće je koristiti i 256 bitni upotrebom lokalne ili domenske sigurnosne politike te unosa u registar,
- podržana je AES enkripcija za dokumente formata Open XML prethodnih inačica Microsoft Office sustava ako su ti dokumenti stvoreni upotrebom Office 2007. Međutim dokumenti pohranjeni u binarnom formatu kriptirat će se algoritmom RC4 kako bi bili sukladni s prethodnim inačicama paketa Microsoft Office,
- AES enkripciju podržavaju operacijski sustavi Windows Server 2003, Windows XP SP2 i Windows Vista. AES je funkcionalnost ugrađena u operacijski sustav,
- razina zaštite koju pruža AES enkripcija ovisi o jačini zaporke koja se koristi za zaštitu dokumenta. Preporuča se upotreba složenih zaporki najmanje duljine 8 znakova te koje uključuju mala i velika slova, brojeve i posebne znakove,
- Microsoft Office 2007, ne uvjetuje složenost zaporke već korisnici sami trebaju znati da je potrebno stvoriti složenu zaporku,
- Microsoft Office 2007 ne uvjetuje da korisnici moraju kriptirati svoje dokumente.

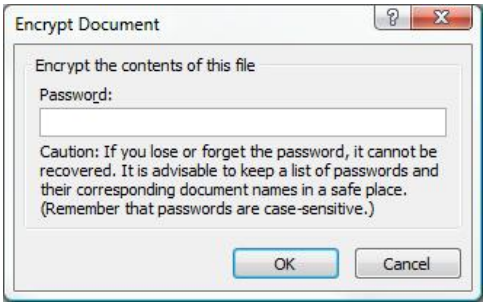
Važno je napomenuti da postoje dvije mogućnosti za dodavanje zaporki na Office 2007 dokumente. Jedan izbor omogućuje kriptiranje dokumenta upotrebom zaporke – *Password to open* funkcionalnost. Drugi izbor ne koristi enkripciju. Osmišljena je tako da ovlaštene osobe mogu mijenjati dokument, no ne čini dokument zaštićenim. Ta funkcionalnost nazvana je *Password to modify*.

Primjer kriptiranja dokumenta u sustavu Microsoft Office 2007 prikazan je na sljedećoj slici:



Slika 5. Primjer kriptiranja dokumenta u Office 2007.
Izvor: Tech Republic

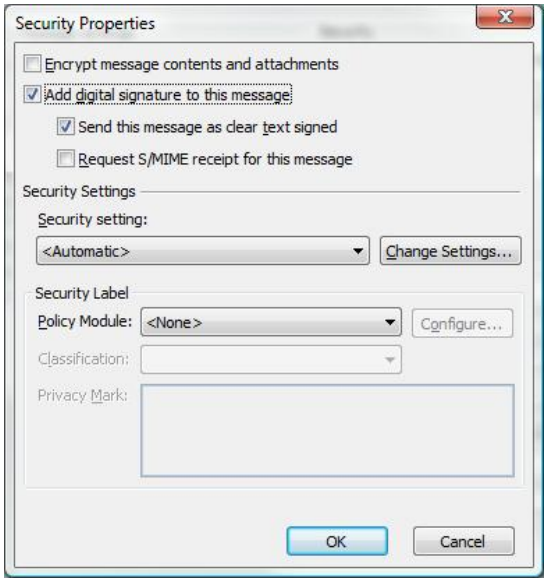
Nakon odabira načina kriptiranja dokumenta od korisnika se traži da unese zaporku za koju se preporuča da se koriste velika i mala slova, brojevi i posebni znakovi.



Slika 6. Unos zaporke.
Izvor: Tech Republic

Nakon unosa zaporke dokument je zaštićen zaporkom i kriptiran. Dokument je moguće sačuvati u formatu Office 2007 (.docx, .xlsx, ili .pptx) ili Office 97-2003 (.doc, .xls, ili .ppt).

Sljedeća slika prikazuje postavljanje digitalnog potpisa na dokument u Office 2007:



Slika 7. Dodavanje digitalnog potpisa dokumentu. Izvor: Tech Republic

4.2. Open Office dokumenti

Dokumenti stvoreni programskim paketom Open Office su zapravo ZIP arhive sa ekstenzijama .odt i .ods umjesto .zip. ZIP arhive sadrže komprimirane podatke o dokumentu. Dekomprimiranje Open Office datoteka otkriva da sadrže nekoliko XML datoteka od kojih je najvažnija content.xml. Kada je dokument zaštićen zaporkom, sve XML datoteke arhive imaju isto ime, ali njihov je sadržaj na prvi pogled slučajni niz znakova zbog toga što su kriptirani. Postupak kriptiranja uključuje sljedeće korake:

1. Stvara se SHA-1 sažetak zaporke dugačak 20 okteta koju je korisnik postavio i dodaje se arhivi.
2. Generator slučajnih brojeva se inicijalizira s trenutnim vremenom.
3. Generator slučajnih brojeva se koristi za stvaranje slučajnog 64-bitnog inicijalizacijskog vektora za stvaranje ključa i dodatka (tzv. *salt* dodatak) za svaku datoteku arhive duljine 16 okteta. Inicijalizacijski se vektor nalazi u datoteci META-INF/manifest.inf.
4. *Salt* dodatak se koristi zajedno sa 160-bitnim SHA sažetkom zaporke kako bi se dobio jedinstven 128 bitni ključ za svaku datoteku arhive. Algoritam koji se koristi za dobivanje ključa je PBKDF2 (eng. Password-Based Key Derivation Function) koji koristi HMAC-SHA-1 [RFC2898] algoritam uz 1024 iteracija.

   PBKDF2 je funkcija za stvaranje kriptografskih ključeva dio je standarda koji se koristi za stvaranje asimetričnih kriptografskih ključeva. PBKDF2 primjenjuje pseudo slučajnu funkciju, kao što je kriptografski sažetak, enkripcija ili HMAC (eng. *Hash-based Message Authentication Code*) na ulaznu zaporku. Uz to dodaje se posebna vrijednost (eng. *salt value*) i proces se ponavlja mnogo puta (najmanje 1000 puta) kako bi se stvorio izvedeni ključ koji se može koristiti kao kriptografski ključ. Dodatni proračuni čine razbijanje zaporke mnogo težim i metoda se naziva ojačavanje ključa. Dodavanje posebne „*salt*“ vrijednosti smanjuje ranjivost na napade rječnikom. Broj iteracija povećava posao koji napadač mora napraviti kako bi izveo napad grubom silom.

   Potrebno je imati prikladnu implementaciju PBKDF2 algoritma koja će ispravno rukovati binarnim zaporkama (zaporkama koje ne sadrže ASCII znakove). Na primjer, važna metoda koja se koristi za rukovanje binarnim zaporkama u programskom jeziku Java, kao što je sljedeća:

```
import javax.crypto.*;
import javax.crypto.spec.*;

SecretKeyFactory keyFactory =
SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1");
PBEKeySpec pbKeySpec = new
PBEKeySpec(password.toCharArray(), salt, 1024, 128);
SecretKey pbKey = keyFactory.generateSecret(pbKeySpec);
byte[] encoded = pbKey.getEncoded();
```

ne funkcionira ispravno sa zaporkama koje ne sadrže ASCII znakove. Funkcija koju koristi Open Office za stvaranje ključa ispravno rukuje binarnim zaporkama.

5. Dobiveni ključ se koristi zajedno sa inicijalizacijskim vektorom kako bi se kriptirala datoteka upotrebom algoritma Blowfish. To je simetrični algoritam koji još uvijek nije razbijen.

Svaka datoteka koja se zaštićuje enkripcijom se komprimira prije provođenja postupka kriptiranja. To omogućuje verifikaciju sadržaja dokumenta koji se stavlja u arhivu. Potrebno je kriptirati datoteke koje su označene zastavicom „STORED". Veličina izvornih datoteka sprema se u posebnu datoteku. Krajnji rezultat je ZIP arhiva s kriptiranim datotekama dokumenta.

4.3. PDF dokumenti

Tipična zaštita PDF (eng *printable document format*) dokumenta je onemogućavanje ispisa dokumenta uz mogućnost pregleda istog na računalu. Postoje dodatne funkcionalnosti koje sprečavaju kopiranje teksta i uređivanje dokumenta. PDF dokumenti primjenjuju zaštitu skrivanjem podataka. Kriptira se sadržaj PDF dokumenta. Kada preglednik PDF dokumenta primi kriptiranu PDF datoteku, on provjerava skupinu zastavica i omogućuje određene operacije (obično pregled), pri tome onemogućujući ostale operacije za koje nije pronašao odgovarajuće zastavice.

PDF dokument se sastoji od niza objekata. Svaki se objekt identificira sa dva broja - broj objekta i broj stvaranja. Postoji i tablica referenci koja sadrži brojeve objekata prema poziciji u dokumentu. Postoji nekoliko tipova objekata, a oni bitni su:

- rječnik – tablica koja povezuje imena sa objektima
- tok (eng. *stream*) – proizvoljan blok podataka, koriste se za datoteke koja sadrže stilove znakova, opise stranica, podatke o slikama i slično.

Svaki dokument ima prateći rječnik koji sadrži reference na stablo objekata stranice sa sadržajem dokumenta. Osim toga može imati i rječnik za kriptiranje. Ako je rječnik za kriptiranje prisutan, odnosno dokument je kriptiran, on sadrži podatke potrebne za dekripciju dokumenta. Slijedi primjer spomenutih rječnika:

```
% Prateći rječnik
    trailer
    <<
        /Size 95          % broj objekata u datoteci
        /Root 93 0 R      % stablo stranice je objekt ID (93,0)
        /Encrypt 94 0 R   % enkripcijski rječnik je objekt ID (94,0)
        /ID [<1cf5...>]   % proizvoljni identifikator datoteke
    >>

    % Enkripcijski rječnik
    94 0 obj
    <<
        /Filter /Standard    % upotreba standardne sigurnosti
        /V 1                 % algoritam 1
        /R 2                 % revizija 2
        /U (xxx...xxx)       % sažetak korisničke zaporke (32 byte)
        /O (xxx...xxx)       % sažetak vlasničke zaporke (32 byte)
        /P 65472             % zastavice za dozvoljene operacije
    >>
    endobj
```

Postoje dvije zaporke - korisnička i vlasnikova. Obično korisnička zaporka nije postavljena, odnosno postavljena je na prazan niz znakova. Tako je svakome omogućeno pregledavanje dokumenta. Ako se PDF datoteka pregledava programom Adobe Acrobat, i korisnik upiše vlasničku zaporku, sve su operacije dozvoljene, uključujuće ponovno kriptiranje datoteke drugačijom zaporkom i sl.

U gornjem primjeru zastavice su 65472 u decimalnom sustavu ili 1111111111000000 u binarnom. Bitovi na pozicijama 0 i 1 su rezervirani i uvijek su 0, 2. bit predstavlja dozvolu za ispis (u ovom slučaju je 0, što znači da ispis nije dozvoljen). Bitovi 3, 4 i 5 su zastavice za izmjenu, kopiranje i dodavanje/uređivanje anotacije (u primjeru su onemogućene). Ostali bitovi (zastavice) su rezervirani.

Postupak stvaranja enkripcijskog ključa je sljedeći:

1. proširivanje korisničke zaporke na veličinu 32 bajta upotrebom nepromjenjivog niza znakova veličine 32 okteta:

```
28 BF 4E 5E 4E 75 8A 41 64 00 4E 56 FF FA 01 08
2E 2E 00 B6 D0 68 3E 80 2F 0C A9 FE 64 53 69 7A
```

   Ako je korisnička zaporka postavljena na *null*, koristi se cijeli niz znakova za proširivanje, inače se spaja korisnička zaporka i spomenuti niz te se uzima prvih 32 okteta.
2. Dodavanje sažetka vlasničke zaporke.
3. Dodavanje dozvola – 32-bitni broj, najmanje značajan bit (eng. LSB - l*east significant byte*) je prvi.
4. Dodavanje identifikatora datoteke. To je proizvoljan niz znakova. Adobe preporuča upotrebu MD5 sažetka različitih podataka o dokumentu kod stvaranja niza znakova.
5. Stvaranje MD5 sažetka od niz znakova dobivenog u prethodna 4 koraka. Prvih 5 bajtova izlaza su ključ za kriptiranje (40 bitni ključ).

PDF datoteke se kriptiraju upotrebom stvorenog ključa RC4 algoritmom.

PDF preglednici provjeravaju zaporku koju upisuje korisnik. Oni pokušavaju dekriptirati dokument upotrebom sažetka korisničke zaporke u ključu datoteke i usporedbom nizom znakova stvorenog u 5 navedenih koraka. Prema postavljenim zastavicama dozvoljavaju i onemogućuju se određene operacije.

Svi objekti u PDF dokumentu su kriptirani. Dekripcija podataka odvija se na slijedeći način:

1. Uzmi ključ datoteke duljine 5 okteta.
2. Dodaj 3 okteta broja objekta po redu tako da je najmanje značajan bit prvi.
3. Dodaj 2 okteta broja stvaranja po redu tako da je najmanje značajan bit prvi.
4. Stvori MD5 sažetak tog niza znakova veličine 10 okteta.
5. Iskoristi prvih 10 okteta dobivenog sažetka kao ključ za RC4 enkripciju kako bi se dekodirao dokument.

4.3.1. Adobe moduli za zaštitu dokumenata

Adobe Acrobat rješenja omogućuju funkcije sigurnosti i zaštite elektroničkih dokumenata, primjenom sljedećih modula:

- *LiveCycle Rights Management ES* i
- *LiveCycle Digital Signatures ES.*

LiveCycle Rights Management ES je modul za stvaranje pravila raspolaganja dokumentom. Omogućuje primjenu sigurnosnih politika na dokumente, određujući tko, što, kada i koliko dugo može raditi s određenim dokumentom, bez obzira nalazi li se on u ili izvan vatrozida organizacije. Bitna je mogućnost da autori dokumenta ili ovlaštene osobe mogu mijenjati sigurnosne politike ili opozvati dokument, čak i nakon što je dokument distribuiran i organizacija nema saznanja gdje se on u tom trenutku nalazi. Ugrađene funkcije omogućuju organizaciji da u realnom vremenu prati sve što se događa s njenim dokumentima, bez obzira gdje se nalaze.

Osnovne poslovne funkcije koje se ostvaruju primjenom *Rights Management ES*-a su:

- zaštita intelektualnog vlasništva i povjerljivih informacija pohranjenih u dokumentima,
- nadzor pristupa dokumentima i ograničavanje prava,
- znanje o tome tko je i kada dokument otvorio, ispisao ili izmijenio te
- mogućnost opoziva dokumenta bez obzira gdje se on nalazi.

Zaštita se provodi mehanizmom 256 bitne AES enkripcije. LiveCycle Rights Management ES primjenjiv je na PDF, Microsoft Word, Microsoft Excel i CATIA dokumente.

LiveCycle Digital Signatures ES je modul koji primjenjuje digitalni potpis te certifikacijske i enkripcijske sposobnosti u poslužiteljskom okruženju. Ugrađuje sigurnosne funkcije u bilo koji PDF dokument, bez obzira koji ga je program stvorio. PDF može sadržavati sliku, tekst, zvuk ili video, a pomoću *Digital Signatures ES* se može zaštiti svaki tip informacije koja je pohranjena u PDF dokumentu. Modul stvara certificirane PDF datoteke. Pomoću njega se mogu kriptirati i dekriptirati dokumenti, provjeriti valjanost digitalnih potpisa te digitalno potpisati velika količina PDF datoteka u tzv. *batch* procesima.

5. Zaštita komprimiranih datoteka

Najčešći formati komprimiranih datoteka su ZIP i RAR. Najveća razlika kod kriptiranja između ZIP i RAR formata je ta da ZIP format koristi slabiji algoritam kriptiranja, dok RAR arhive koriste jači AES-128 standard. Ukoliko je potrebno kriptirati važne informacije bolje je koristiti RAR format.

5.1. ZIP arhive

ZIP je format datoteka koje su komprimirane i pohranjene u obliku arhive. ZIP datoteka sadrži jednu ili više datoteka čija je veličina smanjena, odnosno komprimirana. ZIP podržava nekoliko algoritama komprimiranja. Od 2009. godine najčešće korišten algoritam je Deflate. Format je stvorio Phil Katz 1989. godine za PKZIP.

ZIP datoteke uobičajeno imaju ekstenziju .zip, no mnogi drugi programi koriste ZIP format sa drugačijom ekstenzijom. Neki primjeri takvih datoteka su Java JAR datoteke, Mozilla Firefox Add-on (.xpi), id Software .pk3/.pk4 datoteke, OpenDocument format, Office Open XML i drugi.

Najranija inačica specifikacije ZIP formata datoteka je objavljena kao dio PKZIP 0.9 paketa u datoteci APPNOTE.TXT. Katz je objavio tehničku dokumentaciju ZIP formata i učinio ga otvorenim formatom. Specifikacije je također moguće naći na web stranici organizacije PKWARE.

ZIP datoteku identificiraju prisutnost središnjeg direktorija koji se nalazi na kraju datoteke. U direktoriju su pohranjena imena komprimiranih datoteka zajedno sa drugim meta podacima. Trenutno ZIP format podržava sljedeće metode kompresije:

- Shrunk,
- Reduced,
- Imploded,
- Tokenizing,
- Deflated,
- Deflate64,
- BZIP2,
- LZMA (EFS),
- WavPack i
- PPMd.

ZIP podržava jednostavan sustav enkripcije koji se temelji na zaštiti zaporkom i upotrebom simetričnog kriptosustava koji je dokumentiran u ZIP specifikaciji. Poznato je da je u prošlosti zaštita koju su pružale ZIP datoteke imala ranjivosti. Arhive su bile posebno ranjive na napade s poznatim izvornim tekstom. Još jedan nedostatak bio je neprimjereno ostvarenje generatora slučajnih brojeva.

Specifikacije nakon inačice 5.2. podržavaju nove algoritme kompresije i enkripcije (npr. AES). WinZip koristi AES standard koji koriste i programi 7-Zip, XCeed i DotNetZip. PKWARE Secure ZIP podržava algoritme kriptiranja RC2, RC4, DES, Triple DES, digitalne certifikate i enkripciju zaglavlja arhive.

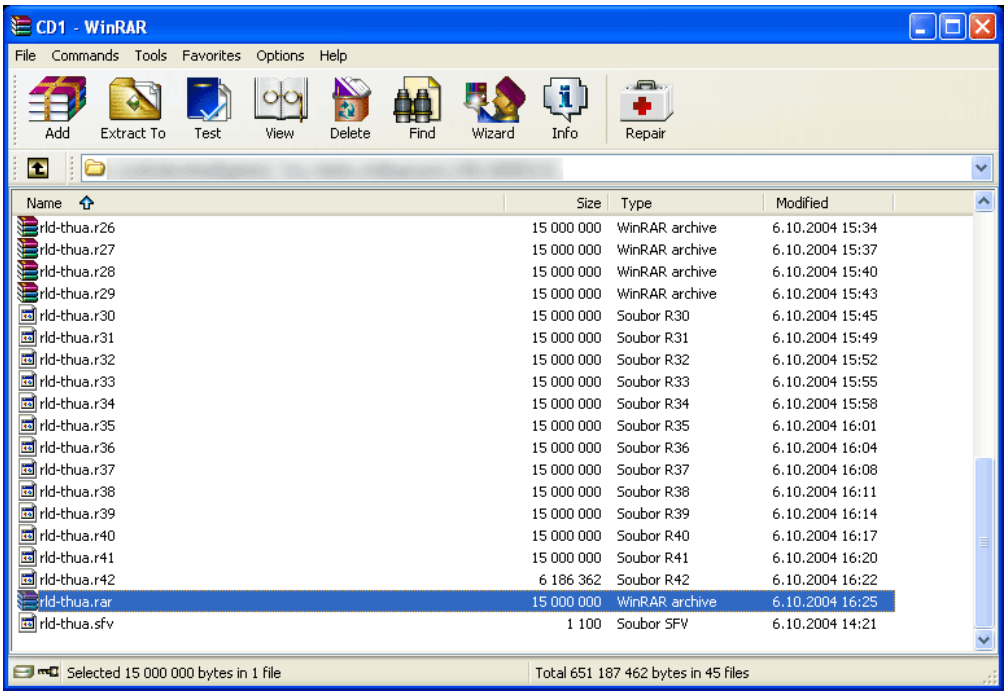
5.2. RAR arhive

RAR (Roshal Archive) je format arhivske datoteke koja podržava komprimiranje podataka, oporavak od pogrešaka te stvaranje više arhiva od jedne velike datoteke. Format je razvio ruski inženjer Eugene Roshal. Ekstenzije koje se koriste su .rar za podatkovnu arhivu i .rev za arhivu koja je nastala oporavkom

od pogreške. Inačica RAR3 se temelji na kompresijama Lempel-Ziv i predviđanju djelomičnim uspoređivanjem (eng. *PPM – prediction by partial matching*).

Postoji tri inačice RAR formata:

- RAR (izvorni),
- RAR2 i
- RAR3 (trenutno u uporabi) – implementirana je u RarLab WinRAR inačici 2.9 i 3.0. Sadrži mnogo promjena u odnosu na prethodne inačice koje uključuju:
  - promjena naziva podijeljenih arhiviranih datoteka,
  - algoritam za kriptiranje je AES sa 128 bitnim ključem,
  - kriptiraju se podaci, kao i zaglavlja datoteka,
  - poboljšani algoritmi komprimiranja koji koristi rječnik veličine 4 MB, PPMII algoritam za podatke datoteka i selektivne algoritme predobrade (eng. selective predprocessing algorithms) temeljene na operacijskom sustavu i tipu izvorne datoteke,
  - proizvoljna mogućnost stvaranja datoteka oporavka od pogreške (eng. recovery volumes) .rev datoteke koje se mogu koristiti za rekonstrukciju datoteka koje nedostaju,
  - podršku za arhive veće od 9 GB,
  - podršku za nazive u Unicode formatu.



Slika 8. Pregled RAR datoteke
Izvor: Releaselog

RAR datoteke se mogu stvoriti upotrebom komercijalno dostupnog programa WinRAR te programskih paketa koji imaju dozvolu onoga koji drži licencu patenta, u ovom slučaju Alexandera Roshala (brata od Eugenea). Jedini besplatan program za stvaranje RAR datoteka je RAR za Pocket PC.

Operacije RAR kompresije su sporije od algoritama koje koristi ZIP, ali ostvaruju bolju kompresiju.

Kriptirane RAR datoteke moguće je napasti upotrebom grube sile, no složenost napada je 2^{128}, što je iznimno velik broj i s današnjim računalima neostvariv u realnom vremenu.

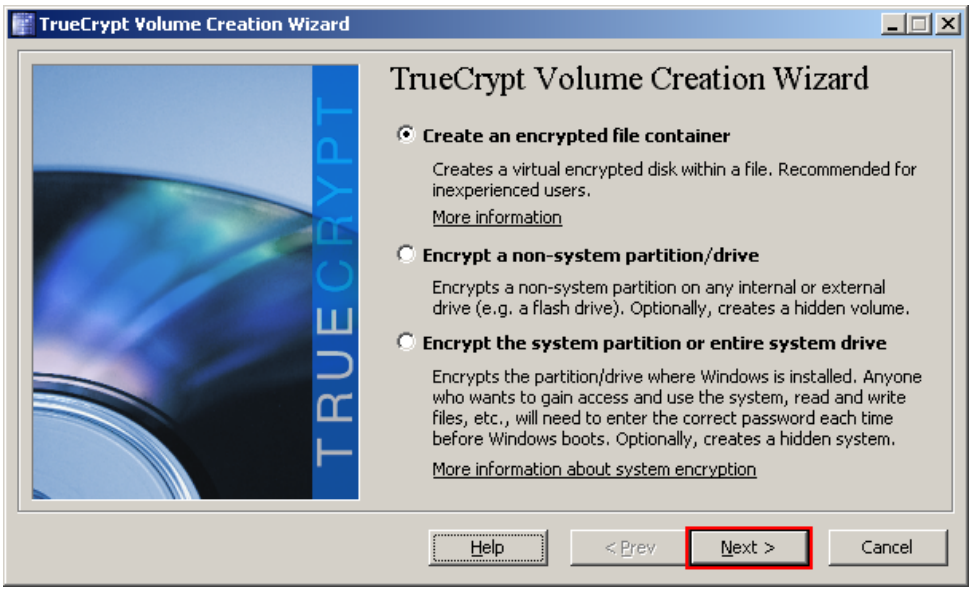
6. Zaštita podataka na disku

Postoje programski paketi koji kriptiraju čitav tvrdi disk računala. Jedan takav programski paket je TrueCrypt, koji se koristi za održavanje i enkripciju diskova tokom njegove upotrebe (eng. on-the-fly). To znači da se podaci automatski kriptiraju ili dekriptiraju prije nego što se učitavaju za prikaz ili spremaju (bez sudjelovanja korisnika). Niti jedan podatak pohranjen na čvrsti disk ne može se pročitati bez odgovarajuće zaporke ili ključa za dekriptiranje. Cijeli datotečni sustav je kriptiran, što uključuje imena datoteka, direktorija, sadržaj svake datoteke, slobodan prostor, meta podatke i ostalo.

Datoteke se mogu kopirati na disk priključen u program TrueCrypt na jednak način kao da se kopiraju na ili sa nekriptiranog diska. Datoteke se automatski dekriptiraju u memoriji (*RAM – random access memory*) tokom čitanja ili kopiranja sa kriptiranog TrueCrypt diska. Slično, datoteke koje se pohranjuju ili kopiraju na disk automatski se kriptiraju prije upisa na disk.

Primjerice, neka postoji video datoteka sa ekstenzijom .avi pohranjena na TrueCrypt disku. Ta je datoteka potpuno kriptirana. Korisnik upisuje odgovarajuću zaporku i otvara TrueCrypt disk. Kada korisnik dvostruko klikne na ikonu video datoteke, operacijski sustav pokreće aplikaciju pridruženu ekstenziji video datoteke, kao što je VLC. Program za pregled video datoteke učita samo dio video datoteke s kriptiranog diska u RAM gdje se automatski dekriptira. Dok se prikazuje dekriptirani dio, učitava se sljedeći dio video datoteke u RAM te se proces ponavlja. Ovakav se proces naziva *on-the-fly* enkripcija i funkcionira na jednak način za sve tipove datoteka.

Program nikada ne sačuva dekriptirane podatke na disk, samo ih privremeno sprema u RAM. Čak i kada se otvara disk za pregled, podaci spremljeni na disku su još uvijek kriptirani. Kada se ponovno pokrene operacijski sustav ili se isključi računalo, disk se automatski isključuje i datoteke pohranjene na njemu su nedostupne i još uvijek kriptirane. Čak i kada iznenadno nestane struje, datoteke pohranjene na disku su na sigurnom. Kako bi se ponovno moglo pristupiti datotekama potrebno je priključiti disk u TrueCrypt program i upisati odgovarajuću zaporku ili upotrijebiti odgovarajući ključ dekriptiranja.



Slika 9. Stvaranje kriptiranog diska
Izvor: TrueCrypt

TrueCrypt disk se može kriptirati upotrebom algoritama navedenih u tablici 1.

Algoritam	Izumitelj	Veličina ključa (bitovi)	Veličina bloka (bitovi)
AES	J. Daemen, V. Rijmen	256	128
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128
AES-Twofish		256; 256	128
AES-Twofish-Serpent		256; 256; 256	128
Serpent-AES		256; 256	128
Serpent-Twofish-AES		256; 256;256	128
Twofish-Serpent		256;256	128

Tablica 1. Usporedba algoritama koji se koriste za enkripciju diska.

Kriptiranje cijelog diska predstavlja najvišu razinu sigurnosti koju je moguće postići na operacijskom sustavu jer se kriptiraju baš sve datoteke na računalu.

7. Mogućnosti razbijanja zaštite

Obzirom da se zaštita dokumenata svodi na kriptografske metode kao što su kriptiranje, upotreba zaporki, digitalno potpisivanje, stavljanje digitalnog vodenog žiga te upotreba kriptografskih sažetaka, napadač za razbijanje zaštite može upotrijebiti metode kriptoanalize [10]. Potrebno je napomenuti da ukoliko se koriste neprobijeni algoritmi kriptiranja, napadač ne može ili može vrlo teško zaobilaznim putem probiti enkripciju. Neke od metoda razbijanja zaporki spomenute su već u poglavlju 3.2.1.

Asimetrična kriptografija oslanja se na uporabu dva ključa, jednog privatnog i drugog javnog. Probijanje takvih enkripcija zasniva se na rješavanju složenih matematičkih problema. Na primjer, sigurnost sheme za razmjenu ključeva Diffe-Hellman ovisi o složenosti računanja diskretnih logaritama. Godine 1983. Don Coppersmith pronašao je brži način određivanja diskretnih algoritama (u određenoj grupi) što je dovelo do potrebe za uporabom većih grupa u kriptografiji. Sigurnost algoritma RSA ovisi o složenosti faktorizacije cjelobrojnih brojeva. Godine 1980. bilo je moguće faktorizirati broj od 50 digitalnih znamenki na računalu sa 1012 osnovnih računalnih operacija. Do 1984. godine s istim utroškom računalnih resursa bilo je moguće faktorizirati broj s 75 digitalnih znamenki. Napredak u računarskoj tehnologiji također je značio i brže obavljanje operacija na računalima. Na brzim, modernim računalima stručnjaci su uspjeli faktorizirati brojeve s 150 digitalnih znamenki pa se takva duljina ključa od početka 21. stoljeća, ne smatra dovoljnom za sigurnost algoritma RSA.

Lars Knudsen napravio je podjelu rezultata kriptoanalize dijela podataka prema količini i kvaliteti otkrivenih tajnih informacija na:

1. **Potpuno probijanje** (eng. *total break*) - napadač je otkrio tajni ključ.
2. **Globalna dedukcija** (eng. global *deduction*) - napadač je otkrio funkcijski ekvivalent algoritma za kriptiranje i dekriptiranje, ali ne i ključ.
3. **Lokalna dedukcija** (eng. instance or *local deduction*) - napadač je otkrio dodatne otvorene tekstove (ili kriptirane tekstove) koji ranije nisu bili poznati.
4. **Informacijska dedukcija** (eng. *information deduction*) - napadač dobiva Shannonove informacije (Shannonova entropija – mjera informacija sadržanih u određenoj poruci) o otvorenim tekstovima (ili kriptirane tekstovima) koji ranije nisu bili poznati.
5. **Algoritam koji omogućuje razlikovanje** (eng. *distinguishing algorithm*) - napadač može razlikovati kriptirani tekst od slučajne permutacije.

Uspješna kriptoanaliza donosi mogućnost pregleda tajnih poruka. Jedna od najvažnijih metoda analize napada na funkcije za računanje sažetka poruke je diferencijalni kriptoanalitički napad. Općenito, spomenuti se napad uglavnom koristi za razbijanje kriptiranih blokova teksta. Diferencijalna analiza je u osnovi napad odabranim otvorenim tekstom i oslanja se na analizu razlika između dva otvorena teksta koji su kriptirani istim ključem (u slučaju primjene na sažetke poruke koristi se ista funkcija sažimanja). Diferencijalna kriptoanaliza može koristiti XOR logičku funkciju za otkrivanje razlika među tekstovima. Prvi koji je upotrijebio diferencijalnu kriptoanalizu kao metodu otkrivanja kriptiranog teksta bio je Murphy, a kasnije su metodu unaprijedili E.Biham i A.Shamir, koji su analizirali sigurnost DES algoritma kriptiranja. Oni su opisali diferencijalnu kriptoanalizu kao metodu koja analizira utjecaj određenih razlika u parovima izvornih tekstova na razlike u rezultirajućim parovima kriptiranih tekstova.

7.1. Napadi na digitalne potpise

Napadi na digitalni potpis mogu se podijeliti u dvije osnovne skupine:

- **napadi uz poznavanje ključa** – napadaču je dostupan samo potpisnikov javni ključ,
- **napadi uz pristup porukama** – napadač ima pristup potpisanim porukama.

Napadi uz pristup porukama mogu se podijeliti prema načinu na koji su poruke dostupne napadaču odabrane:

1. Napad na poznate poruke – napadač ima pristup skupu $m_1, \ldots, m_t$ potpisanih poruka koje nije on odabrao.
2. Napad na generički odabrane poruke – napadač prije pokušaja lažiranja potpisa odabire skup poruka i daje ih korisniku na potpis. Prilikom odabira poruka napadač nema uvid niti u jedan vjerodostojan potpis pa je ovo neadaptivan napad. Izbor poruka ne ovisi o korisnikovom javnom ključu pa se napad naziva generičkim – jednak skup poruka koristi se za napade na potpise svih korisnika.

3. Usmjereni napad na odabrane poruke – napadač odabire poruke na temelju korisnikovog javnog ključa, ali bez uvida u vjerodostojan potpis. Ovo je također neadaptivan napad, ali nije generički jer je usmjeren na pojedinog korisnika.
4. Adaptivan napad na odabrane poruke – napadač korisniku na potpis daje poruke odabrane na temelju korisnikova javnog ključa i prethodno pribavljenih potpisa.

Nabrojani tipovi napada poredani su prema rastućoj težini. Najopasniji su adaptivni napadi na odabrane poruke, a to je ujedno i najčešća vrsta napada zbog toga što se korisnici žele pouzdati u korišteni sustav digitalnog potpisa toliko da mogu bez straha potpisivati proizvoljne dokumente.

7.2. Napadi na digitalne vodene žigove

Digitalni vodeni žig može biti izmijenjen namjerno ili slučajno. Sustav za detekciju vodenog žiga mora biti sposoban detektirati i izvući vodeni žig nakon izmjene. Kod namjernog napada, napadač ne želi ugroziti kvalitetu slike, ali mu je cilj uništiti žig. Nenamjerni napadi se zbivaju slučajno prilikom prolaska kroz komunikacijski kanal. Slijede vrste napada na vodene žigove:

- **Šum-napad** – može nastati slučajno prilikom slanja slike, no napadač ga može i namjerno provesti dodavanjem manje razine šuma, a da pri tome ne ugrozi kvalitetu slike.
- **Filtriranje** – uništava žig samo u slučaju kada se filtriranjem izbacuju oni dijelovi dokumenta u koje je ubačen vodeni žig.
- **Odsijecanje** – ako jedan dio slike iz nekog razloga nestane, cilj autora dokumenta je taj da može detektirati postojanje žiga iz preostalog dijela slike. Napadač to može iskoristiti u slučaju kada posjeduje samo jedan dio slike. Iz njega želi ukloniti žig koji se neće detektirati ako se veći dio žiga nalazi u dijelu slike koji nedostaje.
- **Kompresija** – svi multimedijalni dokumenti koje se prenose i dijele Internetom na neki način su komprimirani te se prijenosom mogu izgubiti određeni podaci. To je primjer slučajnog napada.
- **Rotacija** – nakon operacije rotacije slike žig je gotovo nemoguće detektirati jer se promijeni raspored prostornih uzoraka.

8. Zaključak

Postoji mnogo vrsta dokumenata koji su u svakodnevnoj upotrebi, a velika većina njih sadrži i osjetljive podatke. Kako ne bi dospjeli u neželjene ruke potrebno je takove dokumente zaštititi. Često se događaju gubici dokumenata zbog slučajnog ili namjernog brisanja, prepisivanja, kvarenja čvrstog diska, krađa i slično. Tvrtke koje su izgubile ili su im ukradeni važni dokumenti sa osjetljivim podacima mogu izgubiti mnogo novaca i izgubiti produktivnost. Prema tome, važno je pristupiti zaštiti dokumenata ozbiljno i spriječiti neovlašten pristup, izmjenu, brisanje i neprimjerenu upotrebu osjetljivih dokumenata.

U dokumentu je opisano nekoliko metoda zaštite dokumenata, a one su:

- upotreba enkripcije,
- upotreba zaporki, odnosno ograničavanje pristupa dokumentima
- digitalno potpisivanje dokumenta,
- upotreba digitalnog vodenog žiga i
- kriptiranje cijelog diska.

Svi uredski alati, kao što su Microsoft Office i Open Office imaju funkcionalnosti zaštite dokumenata navedenim metodama (osim, naravno, kriptiranja cijelog diska). Također, datoteke je moguće komprimirati i te arhive kriptirati te tako zaštititi osjetljive dokumente. PDF dokumenti koriste zaštitu ograničavanjem pristupa, pregleda, ispisa, uređivanja i enkripciju. Iako postoje metode razbijanja zaštite, one se uglavnom temelje na tehnikama kriptoanalize. Ukoliko se ne koristi dovoljno veliki ključ kod kriptiranja datoteka, napadač može grubom silom saznati ključ i otkriti osjetljive podatke. Najjednostavniji napadi su napadi razbijanja zaporki. Pri tome napadači najčešće koriste pogađanje i rječnik zaporki. No takvi napadi ne moraju uvijek biti učinkoviti.

Korisnici mogu na razne načine zaštititi svoje dokumente, no uvijek trebaju biti na oprezu i koristiti preporučene duljine ključeva kod enkripcije i preporučene metode stvaranja zaporki.

9. Reference

[1] Safeguard your Office 2007 files with encryption, document protection, and digital signatures, http://articles.techrepublic.com.com/5100-10878_11-6176764.html, travanj 2007.

[2] Documentation – Encryption, http://nsit.uchicago.edu/docs/encryption/msoffice/, listopad 2008.

[3] Document Encryption in Office 2007 with Open XML, http://blogs.technet.com/gray_knowlton/archive/2008/09/02/document-encryption-in-office-2007-with-open-xml.aspx, rujan 2008

[4] PDF encryption, http://www.cs.cmu.edu/~dst/Adobe/Gallery/anon21jul01-pdf-encryption.txt, srpanj 2001.

[5] True Crypt, http://www.truecrypt.org/, travanj 2010.

[6] OpenOffice Encryption, http://selliott.org/encryption/openoffice, rujan 2008.

[7] Sigurnost elektroničkih dokumenata, http://hsm.hr/hsm/index.php?option=com_content&task=view&id=260&Itemid=52, travanj 2010.

[8] ZIP (file format), http://en.wikipedia.org/wiki/ZIP_%28file_format%29, travanj 2010.

[9] RAR, http://en.wikipedia.org/wiki/RAR, travanj 2010.

[10] Kriptoanaliza, http://www.cert.hr/documents.php?id=392, rujan 2009.

[11] Napad na MD5 protokol, http://www.cert.hr/documents.php?id=376, travanj 2009.

[12] Diffie-Hellman protokol, http://www.cert.hr/documents.php?id=400, prosinac 2009.

[13] Rainbows tablice, http://www.cert.hr/documents.php?id=340, kolovoz 2008.

[14] Algoritmi za izračunavanje sažetka, http://www.cert.hr/documents.php?id=257, rujan 2006.

[15] Digital watermarking, http://en.wikipedia.org/wiki/Digital_watermarking, travanj 2010.

[16] Digitalni potpis, http://www.cert.hr/documents.php?id=275, veljača 2007.