UNIVERZITET U BEOGRADU
MATEMATIČKI FAKULTET

Nadežda Kurdulija

ANALIZA OSETLJIVOSTI DIGITALNOG POTPISA

magistarska teza

mentor:
prof. dr Milan Tuba

Beograd, 2009.

Želela bih da se zahvalim mentoru dr Milanu Tubi, kao i članovima komisije dr Niodragu Živkoviću i dr Vladimiru Filipoviću na nesebičnoj pomoći i uloženom vremenu. Ovaj rad želela bih da posvetim svojoj porodici kao znak zahvalnosti na neizmernoj podršci.

Sadržaj

Spisak slika

Spisak tabela

1. Apstrakt

Problem zaštite informacija postao je aktuelan razvojem računarskih tehnologija, a naročito pojavom Interneta. Ključni problem predstavlja sprečavanje neovlašćenog pristupa zaštićenim informacijama, odnosno, provera identiteta korisnika. U uvodnom poglavlju ovog rada data je kratka istorija kriptografije kao i prikaz problema koji će biti razmatran.

Osnovni principi i ciljevi zaštite informacija opisani su u trećem poglavlju. Najpre je definisan pojam kriptosistema, a zatim je navedena klasifikacija različitih napada na kriptosisteme. U okviru ovog poglavlja naveden je primer bezbednosti sistema za daljinsko učenje zbog sve češćih promena i krađa podataka koji se prenose u elektronskoj formi.

U četvrtom poglavlju opisane su pojedine tehnike kriptografije. Pri izboru tehnika koje su prezentovane važno je bilo rukovoditi se time da one oslikaju sve što je od interesa za problem koji se razmatra. S obzirom da su tehnike opisane počev od opštih ka specifičnim, cilj je bio da se stekne slika o mestu koje u oblasti kriptografije pripada digitalnom potpisu.

U sledećem, petom, poglavlju dat je detaljan opis tehnika digitalnog potpisa upotrebom različitih šifarskih sistema. Takođe su razrađeni neki od opštih tipova napada na različite šeme digitalnih potpisa. Na kraju poglavlja izloženi su osnovni principi heš funkcija uz opšti prikaz problema koji ih prate.

U okviru šestog poglavlja izložen je problem rođendanskog napada koji spada u grupu najpoznatijih kolizionih napada na heš funkcije. Centralni deo ovog poglavlja predstavljaju teoreme koje definišu potrebne uslove da bi se obezbedila otpornost regularnih heš funkcija na koliziju.

Kroz nekoliko primera u sedmom poglavlju izložen je generalni pristup konstrukciji i analizi neregularnih heš funkcija. Kroz navedene primere obrađena je analiza rođendanskog napada i potrebni uslovi za ostvarenje kolizije u slučajevima kada neregularna heš funkcija ne zavisi od specifično odabranog algoritma.

U osmom poglavlju, kao zaključak, dat je rezime svega urađenog i dalje smernice u istraživanjima.

2. Uvod

Istorijski posmatrano, počeci kriptografije datiraju još iz vremena starog Egipta, pre 4000 godina, kada su korišćeni neki njeni osnovni elementi [Kahn67]. Sama reč kriptografija je grčkog porekla i znači "tajno pisanje". Kriptografija, kao studija matematičkih tehnika koje se odnose na aspekte zaštite informacija, zajedno sa kriptoanalizom, čiji je cilj ugrožavanje sigurnosti informacija, čine osnovu naučne discipline kriptologije [Mene96].

Od trenutka kada je pismo postalo osnovno sredstvo komunikacije, pojavila se potreba za očuvanjem tajnosti sadržaja, pogotovo u vojnim i diplomatskim krugovima. Sa porastom upotrebe računara prilikom obrade i skladištenja podataka, kao i razvojem komunikacionih sistema, šezdesetih godina prošlog stoleća, javni interes za kriptografijom je naglo porastao. Prvobitni zahtevi od strane privatnog sektora odnosili su se na zaštitu sve većeg broja informacija u elektronskoj formi. Početkom 1977. godine usvojeni su prvi standardi u kriptografiji: *U.S. Federal Information Processing Standard* za šifrovanje neklasifikovanih informacija i *Data Encription Standard,* koji su do danas ostali aktuelni.

Najiznenađujući razvoj u istoriji kriptografije desio se 1976. godine kada su Diffie i Hellman objavili *New Directions in Cryptography*. Ovaj rad predstavlja uvod u revolucionarni koncept šifrovanja javnim ključevima, kao i novi metod za razmenu ključeva [Diff76]. Iako u tom trenutku autori nisu imali praktično rešenje za svoj koncept, ova ideja probudila je ogromno interesovanje za novu oblast, pa je u narednom periodu došlo do njene prave ekspanzije. Rivest, Šamir (*Shamir*), i Adleman otkrili su 1978. godine prvo praktično rešenje za predloženi koncept, danas poznato kao RSA. Ovo rešenje je zasnovano na matematičkom problemu faktorizacije velikih brojeva. Kasnije, 1985. godine, ElGamal je ponudio drugo praktično rešenje koje je zasnovano na problemu diskretnih logaritama.

Jedan od najznačajnijih doprinosa dobijenih uvođenjem koncepta javnih ključeva je digitalni potpis. Prvi internacionalni standard za digitalne potpise ISO/IEC9796 usvojen je 1991. godine i bazira se na RSA algoritmu. Nekoliko godina kasnije, 1994. godine, usvojen je i *Digital Signature Standard* zasnovan na ElGamal-ovoj šemi.

Nagli razvoj računarskih tehnologija poslednjih godina, omogućio je da se podaci i informacije obrađuju, prenose i čuvaju u elektronskom obliku. Sa druge strane, ovakav vid razmene podataka doneo je sa sobom i negativne posledice. Krađa informacija, njihova zloupotreba i falsifikovanje postali su prisutniji nego u klasičnim sistemima kominikacija. Poverljivi podaci u velikim računarskim mrežama dostupni su neovlašćenim licima koja ih mogu pročitati ili promeniti što u određenim slučajevima može izazvati veoma negativne posledice. Da bi se obezbedili tajnost, integritet, i druga svojstva vezana za očuvanje bezbednosti informacija koriste se različite kriptografske tehnike. Promena i krađa podataka koji se čuvaju u elektronskoj formi je toliko prisutna, da bi se bez kriptografskih alata za očuvanje bezbednosti informacija bilo kakva ozbiljnija komunikacija ili razmena podataka mogle smatrati besmislenom.

U ovom radu predmet istraživanja je sigurnost neregularnih heš funkcija i njihova otpornost na koliziju. U konkretnom slučaju u pitanju je otpornost na rođendanski napad kao jedan od karakterističnih predstavnika napada grubom silom. Kako se digitalni potpis ostvaruje pomoću heš funkcija, potrebno je proučiti njihove osobine, i na osnovu toga, ukazati na slabosti koje se javljaju prilikom rođendanskog napada. Iako je istraživanje sprovedeno sa ciljem otkrivanja slabosti heš funkcija, dobijeni rezultati uglavnom idu u prilog povećanju sigurnosti heš funkcija u slučaju kolizionog napada.

Osnovna ideja ovog rada postavljena je kroz generisanje i proučavanje neregularnih heš funkcija koje ne zavise od određenog algoritma, što predstavlja nov pristup u odnosu na dosadašnje postupke. Postupak je generalan u tom smislu što je princip na kome se zasniva primenljiv na različite algoritme nezavisno od njihovog mehanizma. Informacije koje se dobijaju iz generalnog pristupa mogu se primeniti na postojećim heš algoritmima.

Kako je navedena klasa neregularnih heš funkcija specifična i nema mnogo reprezenata u dosadašnjim istraživanjima, cilj ovog rada jeste dobijanje rezultata koji će potvrditi slabosti i nedostatke neregularnih heš funkcija u odnosu na regularne funkcije.

3. Bezbednost informacija i kriptosistem

Tokom prvih nekoliko decenija upotreba računara svodila se na razmenu elektronske pošte i deljenje kancelarijskih resursa. Pod takvim okolnostima, bezbednost informacija bila je u drugom planu. Problem je nastao razvojem Interneta, odnosno, razvojem finansijskih, komercijalnih, komunikacionih i drugih aplikacija koje su skoro kompletnu aktivnost najznačajnijih svetskih tokova prebacili u elektronski oblik.

Zaštita informacija može se različito manifestovati u zavisnosti od zahteva koji su postavljeni. Bez obzira na to ko su učesnici u razmeni informacija, neophodno je obezbediti puno poverenje da će ciljevi koji se odnose na zaštitu informacija biti ispunjeni.

3.1. Osnovni bezbednosni ciljevi zaštite informacija

Bezbednosni problemi mogu se grubo svrstati u četiri tesno povezane kategorije koje kriptografija treba da obezbedi [Tane04], [Mene96]:

- **Poverljivost** (eng. *Confidentiality*) obezbeđuje da informacije ne dospeju u ruke neovlašćenih osoba, odnosno da sadržaj informacije može videti samo osoba kojoj je informacija namenjena. Kao sinonim za poverljivost koristi se i termin *tajnost*. Poverljivost se može ostvariti na brojne načine, počevši od fizičke zaštite pa do matematičkih algoritama.

- **Autentikacija** (eng. *Authentication*) omogućava da utvrdimo s kim komuniciramo, t.j, da su učesnici u komunikaciji upravo oni za koje se predstavljaju.

- **Neporecivost** (eng. *Nonrepudiation*) štiti učesnike u komunikaciji od mogućnosti opovrgavanja prethodnih aktivnosti. U slučaju kada dođe do konflikata u kome učesnici iznose protivrečne tvrdnje o prethodnim aktivnostima, neporecivost pruža razrešenje problema jer se svodi na potpisivanje.

- **Integritet** (eng. *Integrity*) ili verodostojnost ne dozvoljava neovlašćene promene informacija koje se šifruju. Na ovaj način detektuju se promene od strane neovlašćenog lica, koje mogu biti izvršene u vidu ubacivanja novih podataka,

brisanja ili zamene postojećih. U najjednostavnijim porukama tipa: Entitetu E isplatiti sumu S, mogu biti promenjeni imena, valute ili iznosi što kao rezultat može izazvati nimalo bezazlene posledice.

Definicija 1.

Kriptografija je studija matematičkih tehnika koje se odnose na različite aspekte zaštite informacija, kao što su poverljivost, autentikacija, neporecivost i integritet.

Pored osnovnih ciljeva zaštite informacija, postoje i drugi ciljevi koji praktično proizilaze iz gore navedenih, kao što su digitalan potpis koji povezuje učesnika komunikacije sa informacijom; autorizacija koja predstavlja prenošenje odobrenja na nekog korisnika; kontrola pristupa koja ograničava pristup određenim resursima.

Opisana problematika posebno je došla do izražaja u savremenim načinima čuvanja i prenosa informacija, mada je postojala i u klasičnim sistemima, ali u mnogo manjoj meri. Zaštita bezbednosti informacija polazi od fizičke zaštite preko različitih oblika zaštite u slojevima računarskih mreža koji se većinom oslanjaju na složene matematičke algoritame šifrovanja.

3.2. Kriptosistem

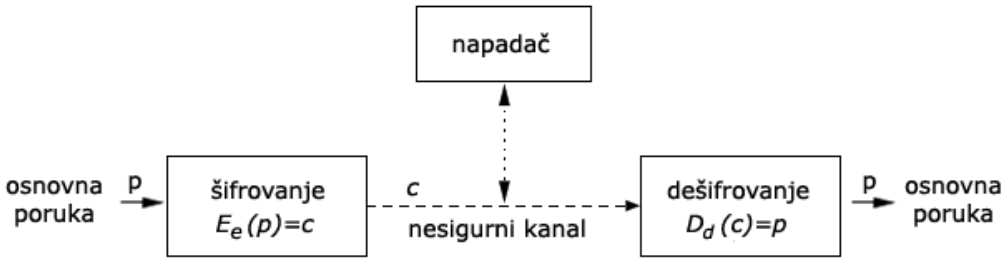
Označimo sa P prostor osnovnih poruka (eng. *plaintext*), sa C prostor šifrovanih poruka (eng. *ciphertext*), i neka je K prostor ključeva (eng. *key*). Funkcijom šifrovanja E_e naziva se bijektivno preslikavanje P u C za svako $e \in K$, dok se funkcijom dešifrovanja D_d naziva bijektivno preslikavanje C u P za svako $d \in K$.

Definicija 2.

Kriptosistem (eng. *cryptosystem*) je petorka (P, C, K, E, D) koja zadovoljava sledeće uslove [Stin95]:

1. P je konačan skup osnovnih poruka
2. C je konačan skup šifrovanih poruka
3. K je konačan skup ključeva
4. Za svako $e,d \in K$ postoji jednoznačno određena funkcija šifrovanja $E_e \in E$ i odgovarajuća funkcija dešifrovanja $D_d \in D$ za koje važi $D_d(E_e(p))=p$, za svako $p \in P$.

Kriptografskim metodama obezbeđuje se privatnost komunikacije između učesnika A i B, kao što je prikazano na *Slici 1*. Učesnik A funkcijom šifrovanja transformiše osnovni tekst u nerazumljiv šifrovan tekst, koji šalje osobi B komunikacionim kanalom, koji može biti zaštićen ili nezaštićen. Funkcijom dešifrovanja učesnik B vraća šifrovan tekst u osnovni tekst. U ranim fazama razvoja kriptografije, postojali su brojni primeri u kojima se poboljšanje zaštite kao i kompletna sigurnost kriptosistema zasnivala na tajnosti funkcija šifrovanja i dešifrovanja [Leht06], [Oppl05]. Otkrivanje ovih funkcija zahtevalo je redizajniranje celog kriptosistema. Da bi se to izbeglo, 1883. godine prihvaćen je Kerkofov princip po kome prostori P, C i K, kao i skupovi funkcija šifrovanja i dešifrovanja E i D moraju biti javni, dok je par ključeva (e,d) tajan.



Slika 1. Slanje i primanje šifrovane poruke

Ugrožavanje ovakvog sistema moguće je samo otkrivanjem para ključeva (e,d), a ostvaruje se iscrpnim pretraživanjem prostora ključeva K. Da bi se obezbedila sigurnost sistema uzima se veliki broj mogućih ključeva koje je nemoguće pretražiti postojećim sredstvima u prihvatljivom vremenskom intervalu.

3.2.1. Funkcije – matematička osnova

Definicija 3.

Funkcija predstavlja pravilo pridruživanja jednog elementa iz skupa X (domen funkcije) drugom elementu iz skupa Y (kodomen funkcije). Za zapisivanje funkcija koristimo oznake kao što je $f: X \rightarrow Y$ ili y = f(x).

Definicija 4.

Funkcija $f: X \rightarrow Y$ zove se surjekcija, ili "na"-preslikavanje, ako svaki element y iz Y predstavlja sliku bar jednog elementa x iz skupa X, odnosno
$(\forall y \in Y)(\exists x \in X)\ f(x) = y$.

Definicija 5.

Funkcija $f: X \rightarrow Y$ zove se injekcija ili "1-1"-preslikavanje, ako važi
$(\forall x_1, x_2 \in X)(f(x_1)=f(x_2)) \Rightarrow (x_1=x_2)$.

Definicija 6.

Funkcija $f: X \rightarrow Y$ je bijekcija ako za svako y iz Y postoji tačno jedno x iz X, takvo da je f(x) = y, odnosno, $(\forall x \in X)(\exists_1 y \in Y)\ f(x) = y$, drugim rečima, f je bijekcija ako je injekcija i surjekcija između ova dva skupa.

3.3. Vrste napada na kriptosistem

Tokom godina, otkriveni su različiti tipovi napada na kriptosisteme. Mete napada mogu biti kriptografski algoritmi i protokoli. U zavisnosti od vrste napadača, može se izvršiti sledeća klasifikacija napada:

- Pasivan napad - u kome napadač nadgleda komunikacioni kanal, čime se ugrožava očuvanje poverljivosti podataka.
- Aktivan napad – kod koga napadač pokušava da obriše ili izmeni poruku koja se šalje komunikacionim kanalom, čime se pored poverljivosti podataka ugrožava i njihov integritet i autentičnost.

Cilj ovih napada je otkrivanje osnovne poruke na osnovu šifrovane, ili još drastičniji, otkrivanje ključa koji se koristi za dešifrovanje. U literature se navode sledeći specijalizovani napadi [Mene96]:

- Napad isključivo šifrovanog teksta *(eng. Ciphertext-only attack*), u kome kriptoanalitičar pokušava da nađe osnovnu poruku, uz pretpostavku da mu je poznata samo šifrovana sekvenca.
- Napad sa poznatim osnovnim tekstom (eng. *Known-plaintext attack*), u kome napadač ima deo osnovne poruke i njoj odgovarajuću šifrovanu poruku.

- Napad izabranog osnovnog teksta (*Chosen-plaintext attack*), u kome napadač izabere osnovnu poruku za koju može stvoriti odgovarajuću šifrovanu poruku.
- Napad prilagodljivog izabranog osnovnog teksta (*Adaptive chosen-plaintext attack*), koji je sličan prethodnom napadu, s tim da izbor osnovne poruke može da zavisi od šifrovanog teksta dobijenog tokom prethodnih napada.
- Napad izabranog šifrovanog teksta *(Chosen-ciphertext attack*), u kome napadač izabere šifrovanu poruku za koju može dobiti odgovarajuću osnovnu poruku. Jedan od načina za sprovođenje ovakvog napada jeste mogućnost pristupa opremi za dešifrovanje, ali ne i ključu za dešifrovanje koji može biti ugrađen u opremu. Cilj ovog napada je dobijanje osnovne poruke iz proizvoljne šifrovane poruke bez upotrebe opreme.

3.4. Sigurnost algoritama

Kriptografski algoritmi pružaju različite nivoe sigurnosti, u zavisnosti od toga koliko ih je teško provaliti. Ukoliko je cena provaljivanja viša od vrednosti šifrovanih podataka, ili ukoliko je vreme za provaljivanje algoritma duže od vremena tokom kojeg je neophodno da se sačuva tajnost šifrovanih podataka, može se reći da je algoritam bezbedan.

Svakodnevni razvoj računarskih tehnologija povećavaju mogućnost novih otkrića u oblasti kriptoanalize, pa se ni za jedan algoritam ne može reći da je u potpunosti siguran.

Lars Knudsen je klasifikovao sledeće kategorije razbijanja algoritma [Knud94]:

1. Potpuna provala (eng. *total break*), kriptoanalitičar dolazi do tajnog ključa K
2. Opšti zaključak (eng. *global deduction*), kriptoanalitičar nalazi alternativni algoritam C, funkcionalno ekvivalentan algoritmima $D_k()$ ili $E_k()$, a da pri tom nema ključ K.
3. Trenutni (lokalni) zaključak (eng. *instance deduction, local deduction*), kriptoanalitičar dolazi do osnovne poruke presretnute šiftovane poruke, pri čemu osnovnu poruku ne dobija od legitimnog pošiljaoca.
4. Zaključak na osnovu informacije (eng. *information deduction*), kriptoanalitičar dolazi do neke informacije o ključu ili osnovnoj poruci koje nije dobio direktno od pošiljaoca poruke i koje nije imao pre kriptografskog napada.

Ukoliko bez obzira na broj šifrovanih poruka koje kriptoanalitičar poseduje, nema dovoljno informacija za dešifrovanje osnovne poruke, algoritam se može smatrati bezuslovno sigurnim (eng. *unconditionally secure*). Do danas se jedino jednokratna zaštita (eng. *one-time pad*) ne može razbiti čak i sa beskonačnim resursima. Svi drugi kriptosistemi mogu biti razbijeni takozvanim grubim napadom (eng. *brute-force attack*), odnosno, jednostavnim isprobavanjem svih mogućih ključeva, ili napadom isključivo šifrovanog teksta, i proverom da li rezultujući osnovni tekst ima smisla.

Algoritam se smatra računski sigurnim (eng. *computationally secure*), ili snažnim, ako ne može da se provali raspoloživim sredstvima, bilo postojećim ili budućim.
Parametri složenosti napada se određuju kroz:

1. Složenost podataka (eng. *data complexity*), odnosno količina ulaznih podataka potrebna za napad.
2. Složenost obrade (eng. *processing complexity*), odnosno vreme potrebno za izvođenje napada. Ovo često nazivamo radni faktor.
3. Potrebe skladištenja (eng. *storage requirements*), odnosno količina memorije potrebna za izvođenje napada.

Za procenu složenosti napada, obično se uzima faktor čija je vrednost najmanja. Kod nekih napada ova tri faktora su međusobno povezana pa je često potrebno praviti kompromis između ove tri vrednosti, na primer napad može biti brži ukoliko se koristi veći prostor za skladištenje.

Složenost se izražava eksponentom broja 2. Ako je složenost obrade algoritma 2^{128}, onda je potrebno 2^{128} operacija za njegovo razbijanje. Ako pretpostavimo da postoji dovoljno brz računar da izvede milion operacija svake sekunde, i ako se postavi milion paralelnih procesora za obavljanje zadatka, još uvek će biti potrebno više od 10^{19} godina za otkrivanje ključa.

Složenost napada na algoritam je konstantna dok se ne osmisle bolji napadi, ali brzina računara nije i stalno se povećava. Kompjuterska tehnologija je u proteklih pola veka zabeležila neverovatan napredak, pa nema razloga za pomisao da se takav trend neće nastaviti. Mnogi kriptoanalitički napadi su savršeni za paralelno povezane mašine: zadatak se može razbiti na milijarde delova, a procesori ne moraju da komunicaraju između sebe. Proglasiti algoritam sigurnim samo zato što je nepraktičan za provaljivanje s današnjom tehnologijom nije ispravno i veoma je riskantno. Dobri kriptosistemi su dizajnirani tako da ih je nemoguće provaliti čak i kada se uzme u obzir razvoj kompjuterske tehnologije još mnogo godina u budućnosti.

3.5. Sistemi za daljinsko učenje

Iako je računarska industrija još uvek mlada u poređenju sa drugim industrijama, računari su zabeležili neverovatan napredak za srazmerno kratko vreme. Ideja po kojoj jedan računar može da zadovolji sve potrebe pojedinca ili organizacije, zamenjena je modelom u kome posao obavlja veći broj zasebnih, ali međusobno povezanih računara. Izrazom „računarska mreža" označava se skup nezavisnih računara, međusobno povezanih jedinstvenom tehnologijom [Tane04]. Za dva računara se kaže da su povezana ako mogu međusobno razmenjivati podatke. Povećan protok informacija i usluga nezamislivo je ostvarivati drugačije osim u elektronskom obliku. Savremeno dinamičko okruženje zahteva nove trendove u različitim oblastima pa tako i u obrazovanju.

Tradicionalini pristup nastavi u današnjim uslovima ima slabosti i nedostatake, pogotovo zbog nedovoljne količine vremena samih korisnika. Uvođenje učenja na daljinu, odnosno, sistema daljinskog učenja (eng. *Distance Learning*, *DL*), kao potpore tradicionalnom školovanju postaje svakim danom sve veća nužnost. Dok je u tradicionalnom sistemu obrazovanja geografska podudarnost predstavljala osnovnu nužnost za obavljanje nastave, danas je to sasvim nebitan detalj. Prema poslednjim podacima Sloan konzorcijuma (eng. Sloan Consortium), preko 3,5 milinona studenata pohađalo je različite online kurseve tokom 2007. godine [Sloa07].

Učenje na daljinu definiše se sledećim osobinama procesa učenja [Stei96]:

- Fizička odvojenost predavača i učesnika tokom većeg dela obrazovnog procesa
- Korišćenje medija u svrhu virtuelnog povezivanja predavača i učesnika, kako bi se nastava mogla izvesti
- Omogućavanje dvosmerne komunikacije između učesnika i predavača.

Američka asocijacija za učenje na daljinu (eng. *The United States Distance Learning Association*) definiše pojam učenja na daljinu kao dostizanje znanja i veština kroz dostavljene informacije i uputstva, primenom različitih elektronskih tehnologija, pri čemu se mora naglasiti vremenska i prostorna razdvojenost predavača i učesnika.

3.5.1. Tipovi učenja na daljinu

Primena informaciono-komunikacionih tehnologija (IKT) dala je obrazovanju novu dimenziju i omogućila razvoj dva tipa obrazovanja na daljinu [Chut89]:

- Sinhrono, kod koga se zahteva istovremeno učešće nastavnika i studenta u obrazovnom procesu, pri čemu se postiže efekat učenja u realnom vremenu
- Asinhrono, kod koga se ne zahteva istovremena participacija nastavnika i studenata. U ovom slučaju student je slobodan da sam organizuje vreme za učešće u nastavi. Asinhroni model je mnogo fleksibilniji od sinhronog, a kao posebna prednost pokazalo se da u nekim slučajevima ohrabruje i podržava formiranje virtuelnih zajednica.

Sistem za učenje na daljinu (eng. *Distance Learning System, DLS*) predstavlja inovativnu tehnologiju plasiranja znanja u službi što kvalitetnijeg obrazovanja. Osim samih računara koji predstavljaju osnovu realizacije ovog sistema, značajno mesto zauzimaju multimedijski sadržaji (zvuk, slika, video, interaktivne animacije) koji se mogu prenositi preko CD i DVD medija ili Internet servisa (primarno World Wide Web). Pomoću Internet servisa ostvaruje se komunikacija koja je ključna za proces elektronskog obrazovanja u obliku foruma, chat servisa, e-pošte, news grupa ili video-konferencija. Upotreba Interneta i primena računara dovela su do poistovećivanja učenja na daljinu sa elektronskim obrazovanjem (eng. *e-learning*).

3.5.2. Prednosti i nedostaci učenja na daljinu

Bez obzira da li je u pitanju tradicionalan ili savremen način obrazovanja, učenje mora biti aktivan, konstruktivan i usmeren proces. Centralni aspekti učenja na daljinu su interaktivnost, individualnost i mogućnost neograničene razmene informacija. Sadržaj koji se nudi učesniku kroz različite sisteme za učenje na daljinu potrebno je prvo na određen način podeliti na manje jedinice koje zajedno čine jedan modul koji se naziva – objekat učenja.

Objekat učenja treba da poseduje sledeće karakteristike [Rodr06]:

1. Mogućnost ponovne upotrebe (eng. *reusability*) – nastavni sadržaj koji predstavlja modul sastavljen od manjih nastavnih jedinica treba da je pogodan za razdvajanje na manje sadržaje i ponovno spajanje u druge kurseve,

2. Interoperabilnost (eng. *interoperability*) – objekti učenja se mogu razmenjivati nezavisno od sistema za učenje koji se koristi i od toga ko im je autor,
3. Trajnost (eng. *durability*) – objekti učenja ostaju upotrebljivi bez obzira na buduće načine razmene i prezentovanja,
4. Dostupnost (eng. *accessibility*) – objekat učenja je dostupan svuda, u svakom trenutku i može se lako pronaći na mreži.

Učenje na daljinu u odnosu na tradicionalni način predavanja sa sobom nosi niz prednosti, ali i neke nedostatke. Osnovna prednost ovog tipa obrazovanja predstavlja fleksibilnost nastavnog sadržaja, ali i samog procesa učenja, pogotovo kada se u obzir uzme činjenica da DL omogućava jednostavan 24-časovni pristup potrebnim informacijama. Na ovaj način, studentu se pruža prilika da izučava predmet nezavisno od vremenske i prostorne udaljenosti u odnosu na predavača, tako da rad postaje individualan. Dok je u tradicionalnom sistemu obrazovanja geografska podudarnost bila nužnost obavljanja nastave, danas je to sasvim nebitan detalj. Veliku prednost predstavlja i mogućnost studenta da odredi svoj tempo rada u zavisnosti od predznanja koje poseduje. Tempo i dinamika rada se prilagođava individui. Gradivo u elektronskom obliku se mnogo jednostavnije pretražuje što omogućuje brže i efikasnije učenje. Kada su ekonomski faktori u pitanju, prednosti učenja na daljinu ogledaju se u uštedi i mogućnosti bolje organizacije radnog vremena.

Veliki nedostatak učenja na daljinu je nemogućnost predavača da studente dodatno aktivira svojim izlaganjem uživo, kao i stalnom dvosmernom komunikacijom. Takođe, pomoć polaznicima često nije moguća u realnom vremenu i u neposrednoj komunikaciji licem u lice. Dodatni problem nastaje zbog teškog ostvarenja interakcije koja postoji u učionici, kada su svi fizički prisutni, a simulacije ne mogu zameniti stvaran fizički rad na realnom problemu. Smanjen društveni kontak predstavlja prilično veliki problem. Naime, postavlja se pitanje koliko je student sam sposoban da održi kontinuitet rada bez direktnog kontakta sa predavačem, pogotovo kada je gradivo teško podeliti u jedinice primerene podučavanju preko računara.

Dodatni problemi javljaju se i zbog nedostatak motivacije korisnika za korišćenje e-learning sistema. Najčešći uzroci nemotivisanosti studenata za korišćenje ovih sistema predstavljaju:

- nepostojanje brze Internet veze,
- manjak inicijative predavača,
- neadekvatan i nedovoljno atraktivan materijal

Uvođenje standarda u e-learning sisteme predstavlja neophodan korak u daljem razvoju ovih sistema. Sagledavanjem trenutno postojećih i implementiranih rešenja učenja na daljinu u obrazovnim institucijama uočena je velika razlika u primenjenim Web aplikacijama. Bez obzira da li su u pitanju besplatni, *open-source,* ili sistemi za učenjenje na daljinu koji se placaju, razlike se pojavljuju u organizaciji kurseva, načinu testiranja i polaganja ispita, kao i tipu postavljenog materijala za učenje. Zbog raznolikosti ovih rešenja nameće se potreba za standardizacijom sistema na međunarodnom nivou. Standardizacija e-learning sistema je neophodna zbog ujednačavanja uslova pri učenju, testiranju, polaganju i ocenjivanju studenata.

3.5.3. Bezbednost sistema za daljinsko učenje

Adekvatna bezbednost svakog sistema za učenje na daljinu ostvaruje se kroz zaštitu podataka od nelegalnih napada i modifikacija, uz istovremeno pružanje maksimalne fleksibilnosti autorizovanim korisnicima. Bezbednost sistema daljinskog učenja ugrožena je na više načina. Kada je zaštita sadržaja od nedozvoljene upotrebe u pitanju, javljaju se dva slučaja:

- Zaštita sadršaja od nedozvoljene upotrebe u slušaju neovlašćenog korisnika
- Zaštita sadršaja od nedozvoljene upotrebe u slušaju autorizovanog korisnika

Iako za većinu sistema osnovni problem predstavljaju neovlašćeni korisnici, čiji je cilj krađa, brisanje ili modifikacija podataka, u sistemima daljinskog učenja ovi problemi često se vezuju i za autorizovane korisnike, najčešće u obliku pokušaja krađe ispitnih testova čime se narušava ispravnost procesa polaganja ispita.

Zaštitom mrežnih komunikacionih kanala sprečava se pristup neovlašćenim korisnicima, pri čemu su tajnost i integritet podataka posebno ugroženi. Tajnost se narušava u slučajevima kada neovlašćeni korisnik nadgleda, odnosno, prisluškuje komunikacioni kanal i na taj način dolazi do poverljivih podataka. Sa druge strane, ukoliko poverljivi podaci postanu dostupni neovlašćenim licima, narušavanje integriteta podataka, odnosno, njihova izmena, u većini slučajeva može imati veoma negativne posledice.

Na prvi pogled može delovati iznenađujuće zašto se javlja potreba za zaštitom podataka od autorizovanih korisnika. Pored osnovnog problema krađe podataka, često se nailazi i na zloupotrebu sadržaja, odnosno korišćenje i modifikacija podataka bez

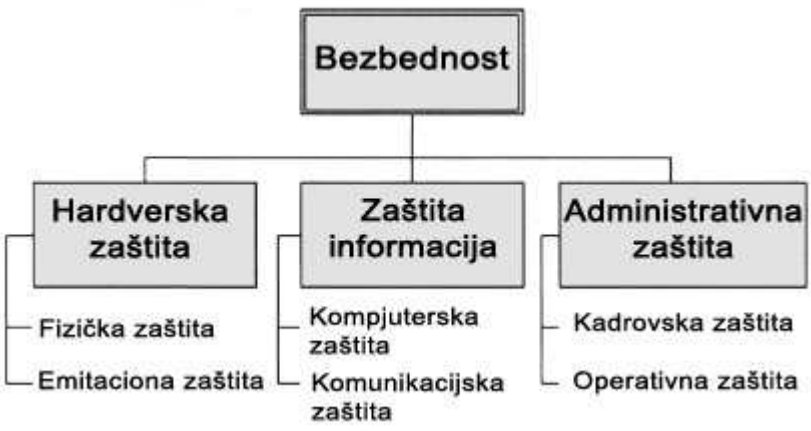
dozvole autora. Autentikaicijom i upotrebom digitalnog potpisa smanjuje se rizik od ovakve zloupotrebe. Autentikacijom se pored provere identiteta korisnika ostvaruje i kontrola pristupa određenim informacijama, dok se digitalnim potpisom proverava integritet sadržaja i pošiljalac.

Logičan nastavak zahteva očuvanja tajnosti i integriteta podataka, predstavlja korak kojim se postiže nemogućnost poricanja, na osnovu čega korisnik ne može poreći da je izvršio neku radnju. Ukoliko, recimo, dođe do brisanja ispitnih rezultata, na ovaj način se može pratiti pristup rezultatima i otkriti počinilac.

Da bi se povećao stepen sigurnosti sistema daljinskog učenja potrebno je ispuniti osnovne zahteve:

- Korisnik mora biti siguran u tačnost podataka
- Sadržaj mora biti zaštićen kako od neovlaščenih tako i od autorizovanih korisnika
- Sadržaj mora biti zaštićen od neautorizovanih promena
- Sadrzaj mora biti zaštićen od uništenja i gubitka podataka

Tradicionalno posmatrano, bezbednost sistema za učenje na daljinu, kao i većine mrežnih sistema, može se ostvariti na tri nivoa [Weip05, Inte06]: hardverskom zaštitom, zaštitom informacija i administrativnom zaštitom, što je ilustrovano na Slici 2.



Slika 2. Osnovni nivoi bezbednosti sistema za učenje na daljinu

Hardverska zaštita (eng. *Hardware security*) obuhvata sve aspekte fizičke zaštite računara (eng. *Physical Security*) uključujući osnovnu zaštitu od oštećenja i krađe do

ekstremnih opasnosti od poplava i zemljotresa. Zahvaljujući emitacionoj zaštiti (eng. *Emanation security)* ostvaruje se zaštita protiv štetnih signala koje emituju elektronski uređaji, prvenstveno elektromagnetnih talasa.

Zaštita informacija (eng. *Information Security*) obuhvata kompjutersku (eng. *Computer Security*) i komunikacijsku zaštitu (eng. *Communication Security*). Kompjuterska i komunikacijska zaštita najčešće su fokusirane na zaštitne kriptografske metode pomoću kojih se obezbeđuje integritet podataka, autentičnost, autorizacija i sl., pri čemu se kao najčešće tehnike koriste digitalan potpis i vodeni žig. Komunikacijska zaštita obezbeđuje sigurnost informacija tokom prenosa podataka i zasnovana je na autentikaciji koja se ostvaruje upotrebom lozinke (eng. *password*) čime se neautorizovanim osoboma onemogućava pristup informacijama.

Administrativna zaštita pokriva problematiku zaštite podataka od strane autorizovanih korisnika, jer se u praksi pokazalo da čovek predstavlja najslabiju kariku u lancu zaštite. U praksi je dokazano da autorizovani korisnici u odnosu na neovlašćene korisnike, predstavljaju mnogo veću pretnju za bezbednost sistema daljinskog učenja. Obično je u pitanju zloupotreba dodeljenih privilegija, intelektualni izazov ili novčana korist.

Razvoj računarskih mreža omogućio je prenos i čuvanje podataka u elektronskom obliku, čime su otvorena vrata razvoju najnovijeg oblika obrazovanja – sistemu daljinskog učenja. Pojava Interneta uslovila je velike promene u komunikacijskoj sferi na društvenim, političkim, obrazovnim, i kulturnim nivoima. Nove Internet tehnologije, zahtevaju zaštićenu Internet komunikaciju, čime se sprečava otkrivanje informacija i njihova zloupotreba od strane neovlašćenih lica.

Jedan od načina da se zaustavi širenje negativnih posledica pronađen je u upotrebi različitih alata za zaštitu podataka. Tokom više stoleća razvoja, savremena kriptografija je postala najmoćniji alat za zaštitu informacija u sistemina daljinskog učenja. Kriptografske metode koje obezbeđuju očuvanje tajnosti, autentikaciju, neporecivost i integritet podataka predstavljaju jedno od glavnih sredstava za sprečavanje neautorizovanog pristupa poverljivim podacima. Digitalni potpis kao kriptografska tehnika kojom se dokazuje autentičnost pravnih, finansijskih i drugih elektronskih dokumenata, zauzima sve značajnije mesto u savremenom dinamičkom okruženju.

4. Klase kriptosistema

Od samog nastanka kriptografije osnovni zadatak je predstavljalo obezbeđivanje privatnosti komunikacije između učesnika A i B, preko nesigurnog komunikacionog kanala (telefonske linije, rašunarskih mreža,...), tako da neovlašćeno lice ne može da je ugrozi. Da bi se povećao stepen sigurnosti, kriptosistemi obično sadrže tajne parametre odnosno ključeve. Bez odgovarajućeg ključa narušavanje sigurnosti komunikacionog kanala postaje gotovo nemoguće.

U zavisnosti od vrste ključa koji se koristi, kriptosistemi se dele na dve klase [Leht06]:

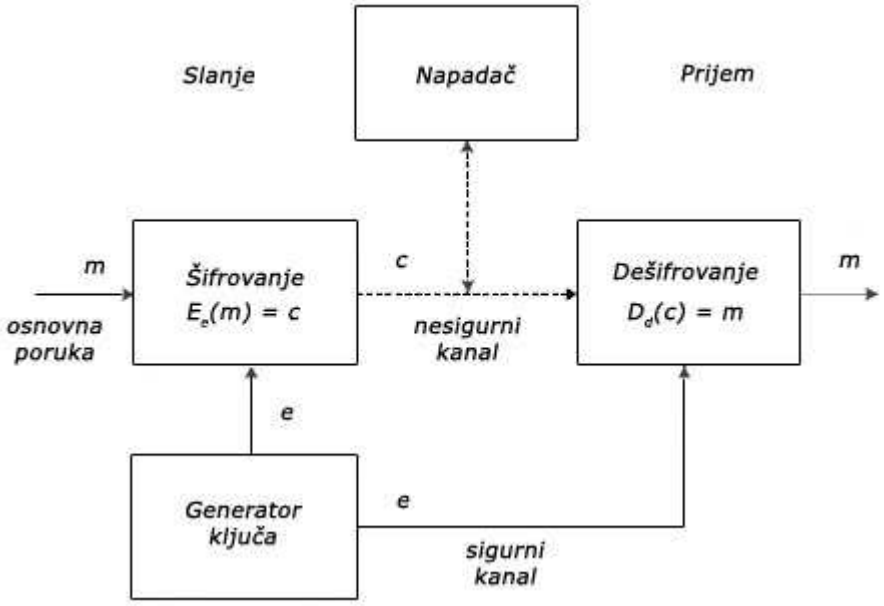
- Kriptosistemi zasnovani na algoritmima za šifrovanje simetričnim ključem
- Kriptosistemi zasnovani na algoritmima za šifrovanje javnim ključem

4.1. Kriptosistemi sa simetričnim ključem

Definicija 7.

Za kriptosistem kažemo da je kriptosistem sa simetričnim ključem ukoliko je za svaki odgovarajući par ključeva (e,d) iz konačan skupa ključeva K, jednostavno izračunati ključ d znajući ključ e, i obrnuto, ključ e na osnovu ključa d.

Pošto se ključevi lako izvode jedan iz drugog, u praksi se obično uzima da je e=d. Samim tim što se računaju jedan iz drugog, par ključeva (e,d) mora biti tajan. Da bi se ostvarila komunikacija između dva učesnika, potrebno je da jedan od učesnika generiše ključ e, a zatim ga pošalje sigurnim kanalom drugom učesniku. Nakon distribucije ključa e oba učesnika mogu da izračunaju tajni ključ d. Na Slici 3. prikazana je komunikacija između dva učesnika u kriptosistemu sa simetričnim ključem.



Slika 3. Slanje i primanje šifrovane poruke u kriptosistemu sa simetričnim ključem

Kriptosistemi sa simetričnim ključevima zadovoljavaju sledeće osobine [Schn96]:

- E_e (p) = c
- D_d (c) = p
- D_d (E_e (p) = p
- d se lako izvodi iz e

pri čemu je $p \in P$ (iz konačanog skupa osnovnih poruka) i $c \in C$ (iz konačanog skupa šifrovanih poruka).

Kriptosistemi sa simetričnim ključem dele se na dve grupe: blok šifarske sisteme (*block ciphers systems)* i sekvencijalne šifarske sisteme (*stream ciphers systems)*.

4.1.1. Blok šifarski sistemi

Kod blok šifarskih sistema osnovna poruka se deli na blokove fiksne dužine n, koji se zatim šifruju jedan po jedan. Šifrovani blokovi su iste dužine kao i odgovarajući ulazni blokovi. Pre pojave računara, kriptografski algoritmi blok šifarskih sistema zasnivali su se na šifrovanju osnovnog teksta slovo po slovo, odnosno, algoritmi su

zamenjivali slova jedno drugim ili ih premeštali. Složeniji algoritmi su radili obe operacije više puta.

Ključni napredak savremenih algoritama je to što rade sa bitovima, a ne sa slovima. Danas se blokovi obično dele na 64 bita mada mogu biti i duži. Tipična dužina od 64 bita dovoljno je velika da spreči osnovne kriptoanalitičke napade, a istovremeno, zadovoljavajuće mala da omogući brzo izvršavanje kriptografskih algoritama. Dve važne klase blok šifarskih sistema su supstitucione šifre i transpozicione šifre.

Kod supstitucionog šifrovanja svako slovo ili grupa slova osnovnog teksta šifruju se tako što se zamenjuju drugim slovom ili grupom slova. Zamenjivanje karaktera ne remeti njihov redosled. U klasičnoj kriptografiji pojavljuju se četiri vrste supstitucionih šifara:

- Obična supstituciona šifra (eng. *simple supstitution*) ili monoalfabetska šifra, kod koje se svako slovo osnovnog teksta zamenjuje odgovarajućim slovom. Ako pretpostavimo da je *A* abeceda od n slova, broj različitih susptitucija je n!. Obične supstitucione šifre ne pružaju adekvatnu zaštitu čak ni u slučajevima kada je skup ključeva K izuzetno veliki. Za dešifrovanje ovakvih tekstova polazi se od osnovnih statističkih svojstva odgovarajućeg jezika, odnosno izračunavanja broja ponavljanja slova, pa se na ovaj način veoma lako razbijaju.
- Homofonična supstituciona šifra (eng. *homophonic substitution cipher*), je slična običnoj supstitucionoj šifri, samo što se u ovom slučaju svako slovo iz osnovne poruke zamenjuje jednim od karaktera iz unapred definisanog skupa karaktera za to slovo. Da bi se sprečili kriptoanalitički napadi zasnovani na frekvenciji slova, potrebno je izjednačiti frekvencije svih slova u datom alfabetu. Broj potencijalnih zamena određenog slova je proporcionalan učestalosti pojavljivanja tog slova. Na primer, frekvencija slova “a” iznosi 8% u odnosu na sva ostala slova engleskog jezika, pa se slovu “a” dodeljuje 8 karaktera koji ga mogu zameniti. Na ovaj način frekvencija svih slova se svodi na 1% u šifrovanom tekstu.
- Poligramska supstituciona šifra (eng. *polygram substitution cipher*) šifruje blokove znakova u grupama. Na primer, “ABA” može odgovarati “RTQ”, “ABB” može odgovarati “SLL”, i slično.
- Polialfabetska supstituciona šifra (eng. *polyalphabetic substitution cipher*) sastoji se od više običnih supstitucionih šifara nad različitim abecedama. Kao rezultat ovakvog šifrovanja dobijamo da se isto slovo osnovnog teksta predstavlja različitim slovima u šifrovanom tekstu. Iako je ovakav način šifrovanja preko 300 godina smatran neprobojnim, za razbijanje je potrebno posedovati dovoljnu dužinu šifrovane poruke, jer će se u tom slučaju neke reči ili delovi reči ponoviti

više puta i biti predstavljene istim karakterima u šifrovanoj poruci. Najpoznatija polialfabetska supstituciona šifra je Vižnerova šifra.

Drugu klasu blok šifarskih sistema čine transpozicione šifre, kod kojih se menja redosled karaktera osnovnog teksta, ali svaki karakter zadržava svoj identitet. Najjednostavniji oblik transpozicione šifre je stubična transpoziciona šifra u kojoj se osnovna poruka ispisuje horizontalno na parčetu papira fiksne širine, a šifrovana poruka se dobija čitanjem vertikalno. Dekriptovanje se ostvaruje zapisivanjem šifrovanog teksta vertikalno na papiru iste širine. Pošto su slova u šifrovanoj poruci ista kao i u osnovnoj poruci analizom učestalosti slova šifrovanog teksta, kriptoanalitičar primenom različitih tehnika može da odredi pravilan raspored slova i time otkrije osnovnu poruku. Obrada šifrovane poruke drugom transpozicionom šifrom u velikoj meri povećava sigurnost. Pojavom savremenih računara, transpozicione šifre se veoma lako otkrivaju ma koliko komplikovano izgledale.

Supstitucione šifre su mnogo zastupljenije od transpozicionih šifara zato što algoritmi zasnovani na transpozicionim šiframa zahtevaju dosta memorije, što može izazvati ograničavanje dužine osnovne poruke.

Iako je danas na raspolaganju veliki broj blok šifarskih sistema, ne postoji sistem koji idealno odgovara svim zahtevima. Razlog za to je u velikom broju zahteva koji se postavljaju u praktičnim aplikacijama kao što su prevelika potreba za procesorskom moći i količinom raspoložive memorije. Najpoznatiji blok šifarski sistemi koji su i danas u upotrebi su DES (eng. *Data Encryption Standard*), Triple Des, AES (eng. *Advanced Encryption Standard*), IDEA (eng. *International Data Encryption Standard*), RC5 (eng. *Rivest Cipher 5*) i dr.

4.1.2. Sekvencijalni šifarski sistemi

Sekvencijalni šifarski sistemi predstavljaju veoma važnu klasu simetričnih algoritama za šifrovanje koji su dizajnirani tako da budu vrlo brzi, čak brži od blok šifarskih sistema. Za razliku od blok šifarskih sistema u kojima se šifruju grupe karaktera odnosno blokovi osnovne poruke fiksnim tajnim ključem, u sekvencijalnim šifarskim sistemima šifruju se individualni karakteri korišćenjem ključa koji se menja tokom vremena. Veća brzina prilikom izvršavanja sekvencijalnih šifarskih algoritama postiže se na taj način što se ne šifruju blokovi podataka, već najmanji delovi osnovnog teksta - bitovi. Ovi algoritmi obično rade na principu da se uporedo sa ulaznim osnovnim tokom

podataka generiše takozvani tok podataka ključa (eng. *keystream*) koji predstavlja sekvencu simbola iz prostora ključeva K, tj. $e_1e_2e_3....e_i \in K$. Tok podataka ključeva se generiše slučajnim postupkom, ili pomoću nekog algoritma za generisanje toka podataka ključa. Osnovna poruka $p_1p_2p_3...$ šifruje se primenom, obično vrlo jednostavne, funkcije šifrovanja u skladu sa odgovarajućim tokom podataka ključa. Tako se dobija šifrovana poruka c1c2c3... gde je $c_i = E_{ei}(m_i)$. Dešifrovanje se ostvaruje inverznim ključem d_i pri čemu je $D_{di}(c_i) = m_{i.}$

Sekvencijalni šifarski sistemi se klasifikuju u dve grupe: sinhrone (eng. *synchronous*) i asinhrone (eng. *asynchronous*). Ukoliko se tok podataka ključa generiše nezavisno od osnovne i šifrovane poruke šifarski sistem se naziva sinhronim. Primalac i pošiljalac u ovom sistemu moraju koristiti isti ključ i biti sinhronizovani. Ako se tokom prenosa izgubi sinhronizacija usled umetanja ili brisanja nekih karaktera, neophodno je izvršiti resinhronizaciju da bi se ponovo uspostavila komunikacija između učesnika. Gubitak sinhronizacije često ukazuje na prisustvo i olakšava detekciju napadača. Ukoliko se tokom prenosa u šifrovanoj poruci promeni neki karakter, to neće uticati na dešifrovanje ostalih karaktera šifrovane poruke. Ipak, ovo može imati i negativne posledice. Ukoliko napadač promeni šifrovanu poruku tako da ona ima smisla u odnosu na osnovnu poruku, primalac te izmene ne može da otkrije. U ovim sistemima je potrebna autentikacija kao i garancija integriteta podataka.

Asinhroni sistemi su oni u kojima se tok podataka ključa generiše u zavisnosti od ključa i fiksnog broja prethodnih simbola šifrovane poruke. Za razliku od sinhronih sistema, asinhroni sistemi omogućavaju automatsko uspostavljanje sinhronizacije nakon umetanja ili brisanja karaktera tokom prenosa poruke. To je omogućeno time što se u postupku dešifrovanja koristi samo određen broj prethodnih karaktera šifrovane poruke. Glavni nedostatak automatske sinhronizacije jeste nemogućnost lakog otkrivanja eventualnog napadača. Radi što bolje sigurnosti, učesnici u komunikaciji moraju obezbediti autentikaciju porekla podataka i proveru integriteta podataka.

Vrlo jednostavan primer sinhronog sekvencijalnog šifarskog sistema kod koga se za funkciju šifrovanja koristi XOR operator, odnosno isključiva disjunkcija, predstavlja Vernamova šifra. Isključiva disjunkcija se nad skupom {0, 1} može definisati kao sabiranje po modulu 2, odnosno, ako su a, b $\in$ {0, 1} onda je $a \oplus b = (a + b) \bmod 2$.

Na ovaj način se šifrovanje *keystream*-om $k_1k_2k_3...$ svodi na $c_i=m_i \oplus k_i$, a dešifrovanje na $m_i=c_i \oplus k_i$, gde je i=1,2,3,….

4.1.2.1. Uslovna verovatnoća

Ako je n ukupan broj mogućih ishoda jednog eksperimenta, koji su podjednako verovatni, a n(B) broj ishoda u kojima se realizuje događaj B, tada je verovatnoća događaja B jednaka

$$P(B) = \frac{n(B)}{n}$$

Neka je n(AB) broj mogućih ishoda koji dovode do realizacije oba događaja A i B. Verovatnoća realizacije i događaja A i događaja B je

$$P(AB) = \frac{n(AB)}{n}$$

Međusobna veza događaja A i B u teoriji verovatnoće proučava se preko tzv. uslovne verovatnoće. Označimo sa P(A/B) uslovnu verovatnoću realizacije događaja A pod uslovom da se realizovao događaj B. Uslovna verovatnoća događaja A/B jednaka je

$$P(A/B) = \frac{n(AB)}{n(B)}$$

Ako se imenilac i brojilac desne strane jednakosti podele sa n dobija se relacija

$$P(A/B) = \frac{P(AB)}{P(B)}$$

preko koje se definiše uslovna verovatnoća.

4.1.2.2. Jednokratna zaštita

Ukoliko se za ključ izabere slučajan niz bitova iste dužine kao osnovna poruka, a zatim izvrši isključiva disjunkcija između ova dva niza, bit po bit, rezultujuća šifrovana poruka otporna je na sve sadašnje i buduće napade. Razlog je u tome što se u šifrovanoj poruci svako slovo pojavljuje približno isti broj puta. Ova metoda poznata je kao jednokratna zaštita (eng. *one-time pad*). Jednokratna zaštita predstavlja savršenu zaštitu (eng. *perfect secrecy*) ukoliko se ključ upotrebi samo jednom.

Definicija 8.

Ako je m osnovna poruka i c odgovarajuća šifrovana poruka, za kriptosistem kažemo da je savršene zaštite (eng. *perfect secrecy*) ukoliko je verovatnoća P otkrivanja osnovne poruke ista bez obzira da li kriptoanalitičar poseduje ili ne poseduje odgovarajuću šifrovanu poruku.

P(m) = P (m/c)

Teorema 1.

Jednokratna zaštita zadovoljava uslov savršene zaštite P(m) = P (m/c)

Dokaz

Neka je prostor osnovnih poruka $\{0,1\}^n$. Neka je P(m) verovatnoća da je osnovna poruka m poslata, P(c) verovatnoća da je šifrovana poruka c uhvaćena i P(k) verovatnoća da je ključ k korišćen prilikom šifrovanja.

Po definiciji je

$$P(m/c) = \frac{P(mc)}{P(c)}$$

Za svaku osnovnu poruku m = (m_1, m_2, m_3,…m_n) i šifrovanu poruku c= (c_1, c_2, c_3,…c_n) postoji tačno jedan ključ K∈*K* za koji važi E_k (m) = c, odnosno

$$K=(m_1 \oplus c_1, m_2 \oplus c_2,\ldots, m_n \oplus c_n)$$

Kako se ključ sastoji od n slučajno izabranih bitova verovatnoća izbora ovog ključa je $\frac{1}{2^n}$, pa je

$$P(c) = \sum_{m\in M} \frac{P(m)}{2^n}$$
$$= \frac{1}{2^n}$$

Slika 4. XOR operacija nad bitovima

Odatle sledi da je

$$P(mc) = P(mk)$$

a kako je izbor ključa nezavistan od izbora osnovne poruke proizilazi da je

$$P(mc) = \frac{P(m)}{2^n}$$

Iz toga sledi

$$P(m/c) = \frac{P(m)}{2^n} 2^n$$
$$= P(m)$$

čime je dokazano da je jednokratna zaštita savršene žaštite. □

U slučaju kada se isti ključ k koristi za šifrovanje dve različite osnovne poruke m_1 i m_2, postoji mogućnost da kriptoanalitičar preko šifrovanih poruka otkrije osnovne poruke. Neka su c_1 i c_2 šifrovane poruke dobijene upotrebom istog ključa k. Ukoliko se XOR operacija primeni na sledeći način $x_1 \oplus k \oplus x_2 \oplus k$ dobija se $x_1 \oplus x_2$. Ako su x_1 i x_2 u ASCII obliku (kodu), analizom učestalosti slova određenog jezika na veoma jednostavan način mogu se otkriti osnovne poruke m_1 i m_2.

Iako teorijski jednokratna zaštita predstavlja savršen način šifrovanja podataka koji se ne može provaliti, u praksi se nažalost pojavljuju nedostaci. Jedan od osnovnih problema vezan je za dužinu ključa, koji ograničava ukupnu količinu podataka koji se mogu šifrovati i poslati. Drugi problem koji se javlja jeste način pamćenja ključa. Pošto je ključ nemoguće zapamtiti, pošiljalac i primalac ga moraju zapisati, čime se otvara mogućnost krađe ključa. Problemi sa jednokratnom zaštitom javljaju se i ukoliko dođe do ispuštanja ili umetanja nekih znakova tokom šifrovanja ili slanja poruke, pri čemu se narušava sinhronizacija šifrovanja i dešifrovanja poruke, a samim tim podaci koji se dobijaju dešifrovanjem gube smisao.

4.2. Kriptosistemi sa javnim ključem

Problem distribucije ključeva koji predstavlja najslabiju tačku simetričnih kriptosistema, rešili su Whitfield Diffie i Martin Hellman 1975. godine predlažući kriptosistem sa javnim ključem. Od tada, započinje intenzivan razvoj ove vrste kriptosistema koji i danas traje.

Definicija 9.

Za kriptosistem kažemo da je kriptosistem sa javnim ključem ukoliko je za svaki odgovarajući par ključeva (e,d) iz konačan skupa ključeva K, neizvodljivo izračunati ključ d znajući ključ e.

Kriptosistemi sa javnim ključevima zadovoljavaju sledeće osobine [Tane04]:

- E_e (p) = c
- D_d (c) = p
- D_d (E_e (p) = p
- d se izuzetno teško može izvesti iz e

pri čemu je $p \in P$ (iz konačanog skupa osnovnih poruka) i $c \in C$ (iz konačanog skupa šifrovanih poruka).

Kriptosistemi sa javnim ključem (eng. *Public-Key Cryptosystems*) ili kriptosistemi sa asimetričnim ključem baziraju se na korišćenju dva ključa:

- javni ključ (eng. *Public Key*), kojim se vrši šifrovanje podataka i
- privatni ključ (eng. *Secret Key*), koji se koristi za dešifrovanje.

Komunikacija između dva učesnika u kriptosistemu sa javnim ključem odvija se tako što učesnik koji želi da primi šifrovanu poruku generiše par ključeva (e,d), odnosno javni i privatni ključ. Zatim javni ključ e šalje komunikacionim kanalom pošiljaocu. Kada primalac dobije šifrovanu poruku c, dešifruje je privatnim ključem d. Javni ključ može biti javno objavljen i dostupan drugim korisnicima, dok privatni ključ uvek mora ostati u tajnosti. Najveća prednost kriptosistema sa javnim ključem u odnosu na kriptosisteme sa simetričnim ključem je u pogledu distribucije ključeva. Princip je zasnovan na činjenici da korisnik koji raspolaže sa javnim ključem može da šifruje poruku, ali ne može da je dešifruje. Samo korisnik koji ima odgovarajući privatni ključ može da dešifruje poruku. Naime, matematički je praktično nemoguće izračunati privatni ključ pomoću javnog ključa. Razlog za to leži u činjenici da se za pravljenje javnog i privatnog ključa koriste tzv. jednosmerne funkcije (eng. *one-way function*) koje se lako računaju u jednom smeru, dok je nalaženje inverznih funkcija veoma teško. Današnji algoritmi za šifrovanje sa javnim ključem zasnivaju se na faktorizaciji velikih brojeva koji se dobijaju kao proizvod velikih prostih brojeva, ili na algoritmima zasnovanim na diskretnim logaritmima.

Ovi kriptosistemi ne zahtevaju postojanje sigurnog kanala prilikom razmene javnih ključeva, pa je na ovaj način omogućena tajna razmena poruka čak i između korisnika koji se nikada nisu sreli. Međutim, u njima je neophodno postojanje autentikacije. Pošto pošiljalac i primalac komunikaciju ostvaruju preko nesigurnog kanala, kriptoanalitičar je u mogućnosti da presretne javni ključ e poslat pošiljaocu, i da mu pošalje ključ e’ koji je sam generisao. Pošiljalac tada šifruje osnovnu poruku ključem

e’ i šalje je primaocu. U nesigurnom kanalu, kriptoanalitičar može presresti šifrovanu poruku, dešifrovati je svojim odgovarajućim privatnim ključem, a zatim je ponovo šifrovanu javnim ključem e poslati pravom primaocu. Stvarni učesnici u komunikaciji ne mogu nikako otkriti uljeza.

Razmena javnih ključeva između korisnika se najčešće vrši preko ovlašćenih organizacija za izdavanje sertifikata (eng. *Certification Authority*). Naime, na Internetu postoji više ovlašćenih organizacija gde korisnici mogu da ostave svoj javni ključ, ili da preuzmu javne ključeve drugih korisnika. Osnovni zadatak sertifikata jeste da poveže javni ključ sa imenom pojedinca ili kompanije.

Glavni nedostatak distribucije javnih ključeva preko ovlašćenih organizacija jeste u tome što korisnik koji postavi svoj javni ključ naglašava svima da će primati šifrovane poruke i na taj način skreće pažnju potencijalnih napadača na sebe.

Kada je dužina ključa u pitanju, kriptosistemi sa javnim ključem koriste znatno duže ključeve nego kriptosistemi sa simetričnim ključem. Dužina od 1024 bita se danas smatra kraćim ključem za asimetrične kriptosisteme. Odgovarajuća dužina ključa je jako bitna prilikom šifrovanja. Pored toga što utiče na stepen zaštite šifrovanih podataka, utiče i na brzinu šifrovanja odnosno dešifrovanja poruke. Zato je neophodno napraviti kompromis između dužine ključa odnosno stepena zaštite šifrovanih podataka i vremena potrebnog za njihovo šifrovanje ili dešifrovanje. Pri određivanju dužine ključa važno je razmotriti koje vrste napada na kriptosistem su najverovatnije, i sa koliko vremena i računarske snage kriptoanalitičar može raspolagati. Presudan uticaj na izbor dužine ključa može imati dužina vremenskog perioda u kome se očekuje da šifrovani podaci ostanu tajni. Sa porastom dužine vremenskog perioda, povećava se i dužina ključa. U svakodnevnim situacijama u kojima se aktuelnost informacija meri danima ili mesecima, dužina ključa od 1024 bita pruža zadovoljavajući stepen zaštite.

Stepen zaštite kriptosistema sa javnim ključem ne zavisi samo od dužine ključa već i od primenjenog kriptografskog algoritma. Najpoznatiji algoritmi koji se primenjuju kada su kriptosistemi sa javnim ključem u pitanju su [Schn96]: RSA, Elgamal i drugi.

4.2.1. RSA asimetrični algoritam

Ime RSA algoritma izvedeno je iz inicijala autora (Ron Rivest, Adi Shamir, i Leonard Adleman) i predstavlja jedan od najjednostavnijih algoritama za razumevanje i implementaciju. Ovim algoritmom obezbeđuje se tajnost i integritet podataka. Njegova sigurnost zasnovana je na problemu faktorizacije velikih brojeva. Za javni i privatni ključ obično se generišu prosti brojevi od 100, 200 pa nekad i više cifara.

Da bi se generisali javni i privatni ključ RSA algoritma prolazi se kroz sledeće korake [Schn96], [Mene96]:

1. Generisati dva velika slučajna prosta broja p i q, približno iste dužine radi što veće sigurnosti,
2. Izračunati proizvod n=pq, i r=(p-1)(q-1),
3. Izabrati slučajan broj e, 1 < e < r, takav da je nzd (e, r) = 1,
4. Koristeći modifikovan Euklidov algoritam odrediti jedinstven ceo broj d, 1<d<r, takav da je $ed \equiv 1 \pmod{r}$.
5. Javni ključ je par (n,e), privatni ključ je d.
6. Brojevi p i q više nisu potrebni i treba ih obrisati.

Da bi se šifrovala osnovna poruka m, potrebno je prvo podeliti poruku na blokove m_i, čija dužina mora biti manja od n. Kako je poruka obično predstavljena kao niz bitova, u praksi je u stvari potrebno pronaći najveći stepen broja 2 za koji važi da je $2^k<n$, a zatim osnovnu poruku deliti u blokove dužine k. Šifrovana poruka c, predstavljena je blokovima c_i, približno iste dužine.

Algoritam šifrovanja je sledećeg oblika

$$c_i = m_i^e \pmod{n}$$

dok je algoritam dešifrovanja oblika

$$m_i = c_i^d \pmod{n}.$$

Neka je poruka m predstavljena kao broj $m \in Zn = [0, n-1]$. Kako je

$$ed \equiv 1 \pmod{r},$$

tada postoji ceo broj k takav da je

$$ed=1+kr.$$

Ako se c_i^d napiše u obliku

$$c_i^d = (m_i^e)^d \pmod n, \text{ odnosno } m_i^{ed} \pmod n,$$

dobija se da je

$$c_i^d = m_i^{k(p-1)(q-1)+1} = m_i\, m_i^{k(p-1)(q-1)} = m_i * 1 = m_i \pmod n,$$

čime je dokazano da algoritam radi.

4.2.1.1. Sigurnost RSA algoritma

Sigurnost RSA algoritma u potpunosti zavisi od pronalaženja efikasnog algoritma za rešenje problema faktorizacije velikih brojeva. Pasivan napadač pomoću javno dostupnih informacija (n, e), faktorizacijom broja n treba da izračuna r i d. Ukoliko izračuna d kriptoanalitičar je u mogućnosti da dešifruje sve osnovne poruke koje su šifrovane privatnim ključem d. Do sada nije pronađen efikasan algoritam za rešavanje ovog problema.

Hardverski i softverski posmatrano, RSA algoritam je nekoliko stotina puta sporiji od DES algoritma. Zbog toga se u cilju poboljšanja efikasnosti šifrovanja RSA algoritmom bira manji eksponent šifrovanja e, npr. e=3. Ukoliko je potrebno istu osnovnu poruku m poslati različitim primaocima, čiji su javni moduli n_1, n_2, n_3, a eksponent e = 3, tada pošiljalac šalje šifrovane poruke oblika $c_i=m^3 \bmod n_i$. Ako je napadač uspeo da presretne šifrovane poruke c_1, c_2 i c_3, korišćenjem Gausovog algoritma napadač može da pronađe rešenje x, $0<x< n_1n_2n_3$, koje zadovoljava kongruencije

$$x \equiv c_1 \pmod{n_1}$$
$$x \equiv c_2 \pmod{n_2}$$
$$x \equiv c_3 \pmod{n_3}$$

Kako je $m^3 < n_1n_2n_3$, koristeći Kinesku teoremu o ostacima, dobija se da je $x= m^3$. Napadač može da rekonstruiše osnovnu poruku m računanjem kubnog korena broja x. Ovakav napad može se izbeći dodavanjem slučajno generisanog niza bitova osnovnoj poruci.

Nekada se može desiti da se isti moduo n koristi za različite parove (e_i, d_i). Tada je moguće da svaki entitet znajući svoj par ključeva, može da izvrši faktorizaciju n, i dobije privatne ključeve drugih entiteta u grupi.

4.2.1.2. Fermat-ova mala teorema

Teorema 2.

Neka je a prirodan broj i p prost broj, pri čemu a nije deljivo sa p, tada je

$$a^p \equiv a \pmod p, \text{ odnosno}$$
$$a^{p-1} \equiv 1 \pmod p$$

Dokaz.

Ostatak pri deljenju prirodnog broja m sa n može uzeti vrednost iz skupa (0,1..., m-1). To znači da za prirodan broj a postoji tačno p-1 različitih mogućih vrednosti pri deljenju po modulu p:

$$a \equiv 0 \pmod p \text{ ili}$$
$$a \equiv 1 \pmod p \text{ ili}$$
$$:$$
$$:$$
$$a \equiv p-1 \pmod p. \qquad (*)$$

Neka je dat niz $0*a$, $1*a$, $2*a$,... $(p-1)*a$. Tada je svaki od članova niza kongruentan sa tačno jednom vrednošću ostatka po modulu p. Ako pretpostavimo da je

$$i*a \equiv j*a \pmod p$$

to znači da

$$p \mid (i*a - j*a), \text{ odnosno}$$
$$p \mid a*(i-j).$$

Kako a uzima vrednosti iz skupa (0,...,p-1) koje su manje od p, sledi da p | (i-j), odnosno, mora biti $i \equiv j \pmod p$. Primenom jednačina (*) dobija se da je

$$(1a) * (2a) *...* (p-1)a \equiv (1) * (2) *...* (p-1) \pmod p, \quad (**)$$

odnosno, kako je

$$(1a) * (2a) *...* (p-1)a = a^{(p-1)}(p-1)! \qquad (***)$$

iz jednačina (**) i (***) dobija se da je

$$a^{(p-1)}(p-1)! \equiv (p-1)! \pmod{p}.$$

Kako je $(p-1)! \neq 0$, obe strane kongruencije možemo podeliti sa $(p-1)!$, pri čemu se dobija da je

$$a^{(p-1)} \equiv 1 \pmod{p},$$

što je i trebalo dokazati. □

4.2.2. ElGamal asimetrični algoritam

Sledeću moćnu klasu asimetričnih algoritama formulisao je ElGamal 1985. god. Ovaj algoritam u suštini predstavlja varijantu Diffie-Hellman sistema za distribuciju tajnih ključeva javnim kanalima. Matematička osnova algoritma leži u praktičnoj nemogućnosti računanja diskretnog logaritma u konačnim poljima.

Definicija 10.

Neka je $(G, *)$ konačna grupa, $\alpha, \beta \in G$, i ceo nenegativan broj. Neka je $\alpha^0 = e$, $\alpha^i = \alpha * \alpha * \ldots * \alpha$ (i puta). Neka je dalje:

$$H = \langle \alpha \rangle = \{\alpha^i : i \geq 0\}$$

ciklična grupa generisana elementom α. Problem diskretnog logaritma sastoji se u nalaženju jedinstvenog celog broja m, pri čemu je $0 \leq m \leq |H| - 1$, takvog da je $\alpha^m = \beta$. Ukoliko ovakav broj postoji on se naziva diskretnim logaritmom i označava se

$$m = log_\alpha \beta.$$

Kriptosistem koji je predložio ElGamal koristi multiplikativnu grupu $G = Z_p^*$ svih nenultih ostataka po modulu p, pri čemu je α generator grupe Z_p^*, a p dovoljno velik prost broj. U ovom slučaju je uz oznake prethodne definicije G = H.

Za generisanje javnog i privatnog ključa ElGamalovog algoritma potrebno je [Schn96], [Mene96]:

1. Generisati slučajan veliki prost broj p i generator α multiplikativne grupe Z_p^*
2. Izabrati slučajan broj a, takav da je $1 \leq a \leq p-1$, i izračunati $\alpha^a \pmod p$
3. Javni ključ je trojka (p, α, α^a), privatni ključ je a.

Pod pretpostavkom da je p slučajan veliki prost broj i α generator multiplikativne grupe Z_p^* treba izračunati $y= \alpha^a \pmod p$, znajući javni ključ. U sledećem koraku potrebno je izabrati slučajan broj k koji je uzajamno prost sa p-1. Da bi se šifrovala osnovna poruka m treba izračunati

$$c_1 = \alpha^k \pmod p$$
$$c_2 = y^k m \pmod p$$

Par c_1, c_2 predstavlja šifrovanu poruku, koja je dvostruko duža od osnovne poruke. Osnovna poruka m izračunava se dešifrovanjem poruke $C =(c_1, c_2)$, i to na sledeći način [Oppl05]:

1. Prvo se koristeći privatni ključ a formira $a' = p-1-a$
2. Zatim se izračuna

$$\begin{aligned} c_1^{a'} c_2 &\equiv \alpha^{ka'} y^k m \pmod p \\ &\equiv \alpha^{k(p-1-a)} y^k m \pmod p \\ &\equiv \alpha^{(p-1)k} \alpha^{(a)-k} y^k m \pmod p \text{ (Fermatova mala teorema)} \\ &\equiv \alpha^{(a)-k} y^k m \pmod p \\ &\equiv y^{-k} y^k m \pmod p \\ &\equiv m \pmod p \end{aligned}$$

4.2.2.1. Sigurnost ElGamal algoritma

Prilikom korišćenja ElGamal algoritma treba voditi računa da se isti slučajan broj k ne koristi za šifrovanje više različitih poruka. Ukoliko je to slučaj, tada se otkrivanjem jedne osnovne poruke m_1 može dobiti druga osnovna poruka m_2. Neka su redom

$$(c_1,c_2) = (\alpha^k \pmod p, y^k m_1 \pmod p)$$
$$(c'_1,c'_2) = (\alpha^k \pmod p, y^k m_2 \pmod p).$$

šifrovane poruke osnovnih poruka m_1 i m_2. Kako su obe poruke šifrovane istim ključem k, ukoliko kriptoanalitičar poseduje jednu od osnovnih poruka, pomoću jednačine (1) lako dolazi do druge osnovne poruke.

$$m_1/m_2 = c_2/c'_2 \quad (1)$$

U slučaju da više korisnika koristi isti prost broj p i generator α, tada se p i α ne smeju publikovati kao deo javnog ključa. Loša strana ovog algoritma je dužina šifrovanog teksta, koja je dva puta duža od originalnog teksta.

4.2.3. Poređenje kriptosistema sa simetričnim i asimetričnim ključem

Svaki od navedenih kriptosistema ima svoje prednosti i mane, u zavisnosti od potreba korisnika. Od samog nastanka kriptosistema sa javnim ključem vođene su brojne debate oko pitanja koji je kriptosistem bolji.

Kada su kriptosistemi sa simetričnim ključem u pitanju prednosti koje se ističu su sledeće:

1. Laka i praktična implementacija, sa velikom brzinom šifrovanja i dešifrovanja
2. Mala hardverska zahtevnost
3. Upotreba relativno kratkih ključeva
4. Mogućnost kombinovanja više kriptosistema radi dobijanja jače šifre

Nedostaci koji se javljaju su sledeći:

1. Oba ključa moraju biti tajna
2. Potreba za sigurnim kanalom prilikom razmene ključeva
3. Praksa nalaže promenu ključa za svaku sesiju

Prednosti upotrebe kriptosistema sa javnim ključem su:

1. Za razmenu javnih ključeva nije potreban siguran kanal
2. Samo jedan ključ mora biti tajan
3. Ključevi mogu ostati nepromenjeni duže vremena

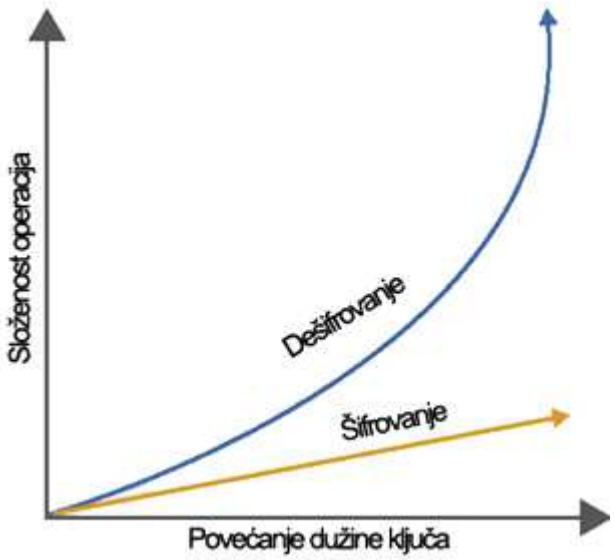
Nedostaci su:

1. Brzina šifrovanja i dešifrovanja je nekoliko stotina puta manja nego kod kriptosistema sa simetričnim ključem
2. Dužina ključa je znatno veća u odnosu na simetrične kriptosistema

Dužina simetričnog DES ključa	*Odgovarajuća dužina RSA ključa*
56 bita	512 bita
80 bita	1024 bita
112 bita	2048 bita
128 bita	3072 bita
192 bita	7680 bita
256 bita	15360 bita

Tabela 1. Odnos dužina simetričnih i asimetričnih ključeva

Iz navedenih poređenja može se primetiti da asimetrične algoritme karakteriše velika sporost u odnosu na simetrične. Razlog za to leži u kompleksnosti faktorizacije velikih brojeva ili izračunavanju diskretnih algoritama. Kod asimetričnih kriptosistema sa porastom dužine ključa složenost dešifrovanja podataka rapidno se uvećava u odnosu na šifrovanje istih podataka, što je grafički prikazano na Slici 5.



Slika 5. Odnost složenosti šifrovanja i dešifrovanja sa porastom dužine privatnog ključa

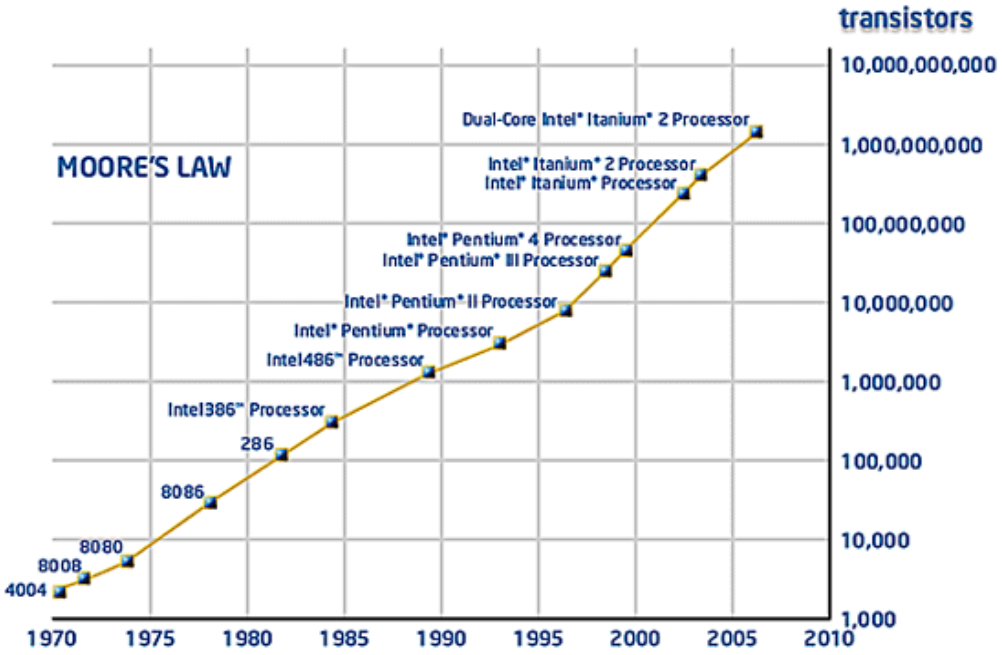
U Tabeli 1. prikazani su odnosi dužine ključeva simetričnih i asimetričnih kriptosistema koji obezbeđuju sličnan stepen sigurnosti prilikom grubih napada [Ecry06]. Bezbednost algoritma zavisi od cene i vremena potrebnih da bi se algoritam provalio. Vrednost većine podataka opada s vremenom, pa je važno da vrednost podataka ostane niža od troškova potrebnih za razbijanje algoritama duži vremenski period. U Tabeli 2. prikazan je odnos važnosti informacije i minaimalne dužine ključa u određenom vremenskom periodu.

Vrsta informacija	*Vremenski period*	*Minimalna dužina simetričnog ključa*
Taktičke vojne informacije	minuti/sati	56-64 bita
Najava novih proizvoda, kamatne stope	dani/nedelje	64 bita
Dugoročni biznis planovi	godine	64 bita
Poslovne tajne	decenije	112 bita
Tajne nuklearnih bombi	> 40 godina	128 bita
Identiteti špijuna	> 50 godina	128 bita

Tabela 2. Odnos dužine simetričnog ključa i važnosti informacija

Ako se uporede rezultati Tabele 1. i Tabele 2. uočava se važnost dužine ključa u terminima zaštite i performanse algoritma. Ukoliko se vremenski period zaštite meri minutima ili satima, nema potrebe za upotrebom ključeva koji obezbeđuju dugogodišnju zaštitu. Koristeći podatke Hermana Rila (*Herman Riel*) [Riel05], tokom 1999. godine za razbijanje RSA-512 bitnog ključa, trebalo je sedam meseci na 300 paralelno povezanih

računara (Pentjum II). Koristeći Murov zakon, (eng. *Moor's low*), u kome se navodi da će se broj pojedinačnih elektronskih elemenata na jednom čipu udvostručiti svakih 18 meseci, lako se dolazi do zaključka da će se za razbijanje RSA-512 bitnog ključa tokom narednih godina vremenski period meriti satima. Na Slici 6. dat je grafički prikaz Murovog zakona.



Slika 6. Grafički prikaz Murovog zakona

Navedene prednosti i mane treba da posluže u pronalaženju i kombinovanju dobrih strana različitih kriptosistema i time omoguće otklanjaje postojećih nedostataka. Elegantno rešenje koje predstavlja kombinaciju kriptosistema sa simetričnim i asimetričnim ključevima omogućava brzo i efikasno šifrovanje poruka privatnim ključem, prednost koju nude kriptosistemi sa simetričnim ključem, i sigurnu distribuciju tog ključa uz identifikaciju pošiljaoca, koja se ostvaruje pomoću kriptosistema sa asimetričnim ključem.

Osnovni koraci prilikom slanja poruke su sledeći:

1. Pošiljalac generiše slučajan privatni ključ – koji se naziva sesijski ključ jer se za svaku sesiju kreira novi privatni ključ
2. Zatim šifruje osnovnu poruku sesijskim ključem koristeći proizvoljan simetrični algoritam

3. Javnim ključem primaoca šifruje sesijski ključ
4. Šalje šifrovanu poruku i šifrovan sesijski ključ primaocu

Kada primalac primi šifrovanu poruku i ključ, prvo dešifruje sesijski ključ pošiljaoca svojim tajnim ključem, a zatim sesijskim ključem dešifruje primljenu poruku. Poruka je u toku prenosa zaštićena sesijskim ključem, koji je poznat samo pošiljaocu koji ga je kreirao. Istovremeno, sesijski ključ je zaštićen tokom prenosa javnim ključem primaoca. Ovakav kriptosistem obezbeđuje siguran kanal za razmenu sesijskog ključa, uz identifikaciju pošiljaoca.

5. Digitalni potpis

Da bi se dokazala autentičnost pravnih, finansijskih i drugih važnih dokumenata u elektronskom obliku, potrebno je obezbediti analogiju stvarnog potpisa rukom. Takva metoda mora biti prvenstveno otporna na falsifikovanje. U osnovi je potreban sistem koji će ispuniti sledeće uslove [Tane04, Abda00]:

1. Primalac može da proveri identitet pošiljaoca
2. Pošiljalac ne može da se ogradi od sadržaja poruke (uslov neporecivosti)
3. Primalac ne može da izmeni primljenu poruku

Sistem digitalnog potpisivanja predstavlja tehniku koja će detaljno biti proučena u ovom poglavlju. Glavna razlika između digitalnog i ručnog potpisa je u tome što digitalan potpis ne može biti konstanta, već funkcija koja zavisi od čitavog dokumenta na kome se pojavljuje. Ukoliko se ne poštuje ovo pravilo, tada digitalan potpis može biti kopiran i dodat na bilo koji dokument u elektronskom obliku. Digitalan potpis treba da potvrdi da je data informacija zaista potekla od određenog entiteta.

Digitalno potpisivanje dokumenata može se ostvariti na različite načine:

1. Pomoću simetričnih šifarskih sistema i arbitratora
2. Pomoću asimetričnih šifarskih sistema
3. Pomoću asimetričnih šifarskih sistema i jednosmernih heš funkcija

5.1. Potpisivanje pomoću simetričnih šifarskih sistema i arbitratora

Treći učesnik u komunikaciji kome veruju obe strane naziva se arbitrator. Pre uspostavljanja komunikacije neophodno je preko sigurnog kanala razmeniti tajne ključeve sa arbitratorom koga predstavlja ovlašćena poverljiva organizacija. Na taj način tajni ključ znaju samo učesnici komunikacije i arbitrator. Broj tajnih ključeva mora biti jednak broju učesnika u komunikaciji. Koraci pri kreiranju digitalnog potpisa su sledeći:

1. Pošiljalac A šifruje osnovnu poruku tajnim ključem K_A i šalje je arbitratoru
2. Arbitrator dešifruje dobijenu poruku tajnim ključem K_A

3. Dešifrovanu poruku uz tvrdnju da je poruku primio od pošiljaoca A, šifruje tajnim ključem K_B
4. Arbitrator šalje poruku primaocu B
5. Primalac dešifruje dobijenu poruku tajnim ključem K_B

Iako na prvi pogled ovakav sistem deluje veoma sigurno, problem se može javiti zbog mogućnosti reprodukovanja poruka od strane uljeza. Da bi se ovaj problem otklonio, pri razmenjivanju šifrovanih poruka treba koristiti vremenske oznake kojima se garantuje svežina osnovne poruke.

5.2. Potpisivanje pomoću asimetričnih šifarskih sistema

Potpisivanje simetričnim ključem zahteva postojanje ovlašćene poverljive organizacije koja ima uvid u sve potpisane poruke. Nažalost ni jedna od ovih organizacija ne pobuđuje potpuno poverenje svih korisnika. Značajan doprinos u rešavanju ovog problema postignut je upotrebom asimetričnih šifarskih sistema. Potpisivanje javnim ključem ne zahteva prisustvo arbitratora, što predstavlja veliku prepreku kod simetričnih šifarskih sistema.

Dodatni zahtev koji u ovom slučaju mora biti ispunjen jeste komutativnost kriptosistema, odnosno, mora važiti:

$$d(e(M) = M, \text{ i}$$
$$e(d(M)) = M$$

Upotrebom privatnog i javnog ključa ostvaruju se svi potrebni uslovi za sistem digitalnog potpisivanja. Kada pošiljalac A želi da pošalje potpisanu poruku primaocu B sledeći koraci su potrebni:

1. Pošiljalac A izračunava digitalan potpis S osnovne poruke P tako što “dešifruje“ osnovnu poruku P svojim privatnim ključem $S=D_A(P)$, a zatim šalje par (P,S)
2. Primalac B proverava da li je poruku P zaista poslao pošiljalac A tako što primenjuje javni ključ pošiljaoca A na potpis S

$$E_A(S) = E_A(D_A(M)) = D_A(E_A\ (M)) = M$$

U principu, svaki algoritam za šifrovanje javnim ključem može se iskoristiti za digitalno potpisivanje, pri čemu je standardni algoritam koji se koristi RSA.

RSA algoritam - U slučaju kada se autentičnost poruke M ostvaruje RSA algoritmom, pošiljalac prvo potpisuje poruku M svojim privatnim RSA ključem d:

$$S = M^d \bmod n.$$

Primalac potpisanu poruku (M,S) proverava javnim RSA ključem pošiljaoca (n,e)

$$M = S^e \bmod n.$$

Iako se upotrebom asimetričnih šifarskih sistema na elegantan način izbacuje prisustvo arbitratora, i rešava osnovni problem simetričnih šifarskih sistema, ovi sistemi ukazali su na nove probleme koji proizilaze iz algoritama i okruženja u kome se radi. Prvi problem nastaje prilikom krađe ili promene tajnog ključa. U tom slučaju nemoguće je potvrditi identitet pošiljaoca. Drugi problem koji se nameće proizilazi iz složenosti algoritama za potpisivanje što kao posledicu ima veliku sporost u odnosu na potpisivanje simetričnim šifarskim sistemima.

5.2.1. Sigurnost i napadi na šeme digitalnih potpisa asimetričnih šifarskih sistema

Zaštita osnovnih karakteristika digitalnog potpisa asimetričnih šifarskih sistema, kao što su jedinstvenost i nemogućnost falsifikovanja potpisa, u najvećoj meri oslanjaju se na sposobnost korisnika da sačuva tajnost privatnog ključa. Široko rasprostranjeno verovanje je da se zaštita tajnog ključa najbolje ostvaruje u slučajevima kada je ključ fizički izolovan na posebnom hardverskom uređaju. Šeme digitalnih potpisa sklone su određenim tipovima napada. U literature se navode sledeći specijalizovani napadi [Taln06]:

- Direktan napad (eng. *Direct attack*) u slučaju kada kriptoanalitičar zna samo javni ključ korisnika

- Napad sa poznatim potpisom (eng. *Known-signature attack*) kada kriptoanalitičar poseduje javni ključ korisnika i nekoliko parova poruka – potpis (M_1, S_1), (M_2, S_2), .. (M_t, S_t)
- Napad izabrane poruke (eng. *Chosen-message attack*) u slučaju kada napadač poseduje javni ključ korisnika i ubedi korisnika da potpiše nekoliko poruka po njegovom izboru (M_1, S_1), (M_2, S_2), .. (M_t, S_t)
- Napad prilagodljive izabrane poruke (eng. *Adaptive-chosen-message attack*), koji je sličan prethodnom napadu, s tim da izbor svake poruke M_i zavisi od potpisa prethodnih poruka.

Cilj ovih napada jeste potpuno razbijanje šeme digitalnog potpisa, čime se napadaču omogućava da za svaku poruku M izračuna odgovarajući digitalan potpis S korisnika. Nakon uspešnog napada ostvaruje se jedno od sledećih razbijanja šeme digitalnog potpisa:

- omogućava napadaču da izračuna potpis bar jedne poruke
- omogućava napadaču da izračuna potpis bar jedne poruke po svom izboru
- napadač može da izračuna potpis svake poruke
- napadač otkriva privatni ključ korisnika

Sigurnost ElGamal algoritam zasniva se na izračunavanju diskretnog logaritma u konačnim grupama, i po svojoj težini može se reći da je ekvivalentan problemu faktorizacije velikih brojeva na čemu je zasnovan RSA algoritam. Ukoliko napadač izračuna diskretni algoritam ili reši problem faktorizacije velikih brojeva, dolazi do potpunog razbijanja (eng. *Total break*) odgovarajuće šeme digitalnog potpisa.

5.3. Digitalni sertifikati

Tokom procesa digitalnog potpisivanja pomoću asimetričnih šifatskih sistema, pored privatnog ključa, potrebno je koristiti i javni ključ entiteta koji šalje poruku. Da bi se to ostvarilo, neophodno je prvo dobiti javni ključ pošiljaoca i potvrditi da je to zaista njegov ključ. Rešenje ovog problema postiže se upotrebom Digitalnih sertifikata. Osnovni zadatak sertifikata jeste da poveže javni ključ sa pojedincem. Sami sertifikati nisu tajni niti zaštićeni. Digitalni sertifikati predstavljaju ličnu kartu entiteta u elektronskom okruženju. Da bi se na Internetu proverili podaci i izdao Digitalni sertifikat pojavile su se kompanije – sertifikaciona tela (*eng. CA - Certificate Authority*), koje imaju ulogu da provere i utvrde nečiji identitet i nakon toga mu izdaju digitalni sertifikat. CA garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom sertifikatu. Zbog toga, ostali korisnici na Internetu ukoliko imaju poverenje u CA mogu biti sigurni da određeni javni ključ zaista pripada korisniku koji je vlasnik tajnog ključa. Na taj način, omogućena je pouzdana razmena javnih ključeva posredstvom Interneta između korisnika koji se nikada nisu sreli, uz mogućnost verifikovanja identiteta korisnika.

Digitalni sertifikat izdat od strane CA mora da sadrži sledeće podatke:

1. Podatke o identitetu korisnika kome je izdat sertifikat, kao što su ime i prezime, E-mail, adresa,…
2. Javni ključ vlasnika sertifikata,
3. Datum do koga važi javni ključ
4. Podatke o entitetu koji je izdao sertifikat, odnosno, o sertifikacionom telu - CA.

5.4. Potpisivanje pomoću asimetričnih šifarskih sistema i jednosmernih heš funkcija

Asimetrični kriptografski algoritmi su veoma neefikasni u praksi, pogotovo kada su u pitanju velike poruke. Da bi se skratio vremenski period potreban za potpisivanje poruka, često se koriste heš funkcije. Bez obzira na dužinu osnovne poruke, heš funkcija obrađuje ulazne podatke u blokovima i kao rezultat vraća 128-bitnu ili 160-bitnu heš vrednost. Potpisivanje dobijene heš vrednosti mnogo je efikasnije i jednostavnije od potpisivanja cele osnovne poruke. Veoma je važno zapamtiti da se na ovaj način potpisuje samo dobijena heš vrednost, a ne ceo dokument.

Kada se heš funkcija koristi kao deo procesa digitalnog potpisivanja, obe strane u komunikaciji moraju heširati osnovnu poruku da bi sa sigurnošću tvrdile da je identitet pošiljaoca i integritet poruke potvrđen.

1. Pošiljalac prvo primenjuje heš funkciju na osnovnu poruku P, pri čemu dobija heš vrednost $h(P) = H$.
2. U sledećem koraku svojim tajnim ključem šifruje samo heš vrednost H i zajedno sa osnovnom porukom P šalje je primaocu.
3. Kada primalac dobije osnovnu poruku i šifrovanu heš vrednost, prvo pravi heš vrednost H_1 dobijene osnovne poruke
4. Zatim javnim ključem pošiljaoca dešifruje potpisanu heš vrednost H.
5. Ako se primljena H i kreirana heš vrednost H_1 slažu, digitalni potpis je validan.

Iako na prvi pogled može izgledati da potreba za duplim heširanjem predstavlja problem i usporava proveru validnosti potpisa, to nije slučaj, jer se heš funkcije brzo izračunavaju. To prakticno znači da svaka promena u sadržaju poruke dovodi do promene potpisa.

Upotreba heš funkcija kao sastavnog dela procesa digitalnog potpisivanja, nosi sa sobom i negativne posledice. Veoma je važno napomenuti da pri izboru heš funkcije treba voditi računa o dužini heš vrednosti koja se dobija heširanjem, da bi se povećala otpornost na koliziju i time povećala sigurnost kriptosistema. U slučaju kolizije najčešće se koristi grub napad radi pronalaženja iste heš vrednosti.

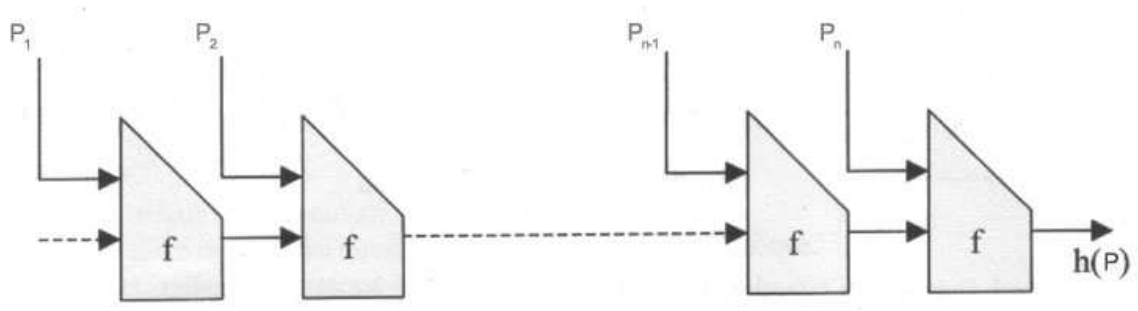
5.5. Heš funkcije

Šifrovanjem osnovne poruke pošiljalac neće obezbediti njen integritet čak i ako ključ nije provaljen. Tehnika kojom se štiti integritet podataka zasniva se na funkciji za jednosmerno heširanje h koja osnovni tekst proizvoljne dužine preslikava u niz bitova fiksne dužine, odnosno, $\{0,1\}^m \rightarrow \{0,1\}^t$, gde je m>t. Funkcija za heširanje ima četiri važna svojstva:

1. Za zadato P lako se izračunava h(P)
2. Za zadato h(P) praktično je nemoguće naći P – jednosmerna funkcija
3. Za zadato P nemoguće je izračunati P' takvo da je h(P) = h(P') – otpornost na koliziju
4. Izmena ulaznih podataka čak i za samo jedan bit daje različit rezultat prilikom heširanja

Jednosmernost i otpornost na koliziju su dva glavna svojstva koje heš funkcija mora da zadovolji da bi se postigla odgovarajuća sigurnost. Otpornost na koliziju je posebno značajna da bi se sprečila krađa digitalnog potpisa. U suprotnom, ukoliko dođe do kolizije dve ili više poruka, digitalni potpis određene poruke koju šalje pošiljalac, može biti zloupotrebljen i dodat na drugu proizvoljnu poruku, bez saglasnosti i znanja pošiljaoca. Heš funkcije su vrlo osetljive i na najmanje promene u osnovnoj poruci, čime se obezbeđuje najbolja zaštita za veće količine podataka.

Jednosmerne heš funkcije su obično iterativne. Osnovna poruka P se deli na blokove podataka $P_1,....P_n$, a zatim se kompresiona funkcija primenjuje na svaki blok i na razultat kompresione funkcije prethodnog bloka. Ovo se nastavlja sve dok se ne dođe do rezultata poslednjeg kompresionog koraka koji predstavlja izlaz h(P). Ideja iterativne heš funkcije data je na Slici 7. Zahvaljujući heš funkcijama uništava se algebarska veza između poruke i njenog potpisa.



Slika 7. Iterativna heš funkcija

Najpoznatije iterativne jednosmerne heš funkcija su MD5 i SHA-1. MD5 je peta u nizu funkcija za heširanje koju je smislio Ronald Rivest. Ova funkcija obrađuje ulazne

podatke u blokovima od 512 bitova i kao rezultat vraća 128-bitnu heš vrednost. Druga poznatija funkcija jeste bezbedni algoritam za heširanje 1 (eng. *Secure Hash Algorithm 1, SHA-1*), koju je razvila agencija NSA. Slično algoritmu MD5, i SHA-1 obrađuje ulazne podatke u blokovima od 512 bitova, ali je rezultujuća heš vrednost dužine 160 bitova. Teorijski posmatrano, za pronalaženje dve poruke koje imaju istu MD5 heš vrednost trebalo bi nekoliko stotina godina čak i u slučaju kada bi se u jednoj sekundi moglo generisati milijardu heš vrednosti. Naravno, kada bi 5000 računara radilo paralelno vreme potrebno za koliziju skratilo bi se na nekoliko nedelja [Tane04]. Algoritam SHA-1 je još sigurniji jer je heš vrednost duža. Rezultati nekih istraživanja pokazuju da je moguće iskoristiti partikularnost algoritma heš funkcija da bi se ubrzao proces pronalaženja iste heš vrednosti.

6. Rođendanski napad

6.1 Rođendanski paradoks

U teoriji verovatnoće rođendanski problem ili rođendanski paradoks odnosi se na određivanje verovatnoće da u proizvoljno odabranom skupu ljudi, bar dvoje imaju rođendan istog dana. Za izračunavanje približne verovatnoće da od n ljudi bar dvoje imaju isti rođendan, polazi se od pretpostavke da svi dani u godini imaju istu verovatnoću rađanja dece, odnosno, može se zanemariti postojanje sezonskih varijacija po kojima se tokom letnjih meseci rađa veći broj dece [Pete98], a kao dodatna stavka navodi se da u grupi ne postoje blizanci.

Uz pretpostavku da je n ≤ N, verovatnoća događaja A, da sve osobe iz proizvoljno izabranog skupa imaju različit datum rođenja, izračunava se na sledeći način:

$$\bar{p}(n) = 1*(1-\frac{1}{N})*(1-\frac{2}{N})*.....*(1-\frac{n-1}{N})$$

$$= \frac{N!}{N^n*(N-n)!}$$

Događaj B, da bar dve osobe imaju isti datum rođenja, predstavlja komplementaran događaj događaju A, da svih n osoba ima različit datum rođenja, pa je verovatnoća događaja B:

$$p(n) = 1-\bar{p}(n)$$

Ukoliko pretpostavimo da je N=365, verovatnoća događaja B dostiže vrednost veću od $\frac{1}{2}$ već u slučaju kada je n=23. U Tabeli 3. dat je pregled vrednosti verovatnoća događaja B koje se dostižu za različite vrednosti broja n.

n – broj slučajno izabranih osoba	*p(n) – verovatnoća da bar dve osobe imaju isti datum rođenja u slučaju kada jeN=365*
10	11.70%
20	41.11%
23	50.70%
30	70.61%
50	97.01%
57	99.00%
100	99.99%
200	99.99%

Tabela 3. Pregled verovatnoća događaja B za različite vrednosti broja n

Iznenađujuća brzina dostizanja visoke vrednosti verovatnoće događaja B, najbolje se može predstaviti grafičkim prikazom. Primenom nejednakosti $e^x > 1+x$ zapis verovatnoće događaja A, odnosno $\bar{p}(n)$, dobija sledeći oblik

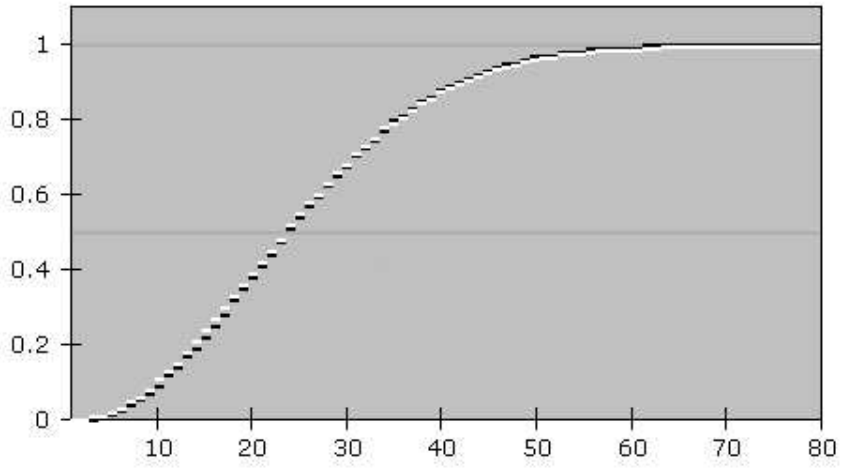
$$\bar{p}(n) < 1 * e^{-1/365} * e^{-2/365} * ..... * e^{-(n-1)/365}$$

$$< e^{(-(n*(n-1))/2)/365}$$

Kako je $p(n) = 1 - \bar{p}(n)$, verovatnoća komplementarnog događaja B je

$$p(n) \geq 1 - e^{-\frac{(n*(n-1))}{2*365}}$$

odnosno $$p(n) \geq 1 - e^{-\frac{n^2}{2*365}} \quad (1)$$



Slika 8. Grafički prikaz funkcije $f(x) = 1 - e^{-\frac{n^2}{2*365}}$

U praktičnim okolnostima osnovni cilj napadača jeste krivotvorenje digitalnog potpisa za poruke koje pošiljalac ne želi da potpiše. Ispitivanjem naizgled istih poruka čija se razlika ogleda u nekoliko bitova, recimo prazno mesto zamenjeno tabom, uočava se velika razlika u odgovarajućim digitalnim potpisima. Da bi ostvario željeni cilj, napadač konstruiše dva niza poruka $\mathcal{M}_1$ i $\mathcal{M}_2$ pri čemu je:

$$\mathcal{M}_1 = \{ M_{1,1}, M_{1,2}, M_{1,3}, ..., M_{1,n} \} \text{ i}$$
$$\mathcal{M}_2 = \{ M_{2,1}, M_{2,2}, M_{2,3}, ..., M_{2,n} \}.$$

Prvi niz $\mathcal{M}_1$ čine poruke izvedene iz osnovne poruke M_1 koju pošiljalac želi da potpiše, i koje su naizgled iste, odnosno razlikuju se u nekoliko zanemarljivih bitova. Drugi niz $\mathcal{M}_2$ čine poruke izvedene iz falsifikovane poruke M_2 koja odgovara napadaču. Suština ovog metoda jeste pronalaženje odgovarajućeg para $M'_1 \in \mathcal{M}_1$ i $M'_2 \in \mathcal{M}_2$ takvog da je

$$h(M'_1) = h(M'_2).$$

Uz prethodno navedene činjenice dolazi se do zaključka da je neuspeh napadača zagarantovan samo u slučaju potpune otpornosti heš funkcije h na koliziju, dok se u svakom drugom slučaju očekuju katastrofalne posledice usled nesigurnosti digitalne šeme.

6.2 Kolizioni napad - rođendanski napad

Opisani rezultati nameću razmatranje metoda kojima napadač pronalazi koliziju za proizvoljnu heš funkciju. Teorijski posmatrano, najpoznatiji kolizioni napad jeste takozvani rođendanski napad. Kao što je prethodno navedeno funkcija za jednosmerno heširanje h preslikava poruke proizvoljne dužine u niz bitova fiksne dužine, odnosno, $\{0,1\}^m \rightarrow \{0,1\}^t$, gde je m>t, što se kraće može zapisati kao h: D $\rightarrow$ R. U slučaju rođendanskog napada, napadač odabira nasumično proizvoljne poruke $x_1, x_2, ..., x_q \in D$ i izračunava $y_i=h(x_i)$, za svako i = 1,....q. Napad se smatra uspešnim ukoliko za različite vrednosti i, j važi da je $h(x_i) = h(x_j)$, pri čemu q predstavlja broj pokušaja.

Lema 1. Neka je $n = 2^{\left\lceil \frac{t+1}{2} \right\rceil}$ i $N = 2^t$, pri čemu je t dužina heš vrednosti. Dokažimo da nejednakost $1-e^{-\frac{(n-1)n}{2N}} > \frac{1}{2}$ važi za t ≥ 5.

Dokaz:

$$1-e^{-\frac{(n-1)n}{2N}} > \frac{1}{2}$$

$$\frac{n(n-1)}{2N} > \ln 2$$

$$\frac{2^{\left\lceil \frac{t+1}{2} \right\rceil}\left(2^{\left\lceil \frac{t+1}{2} \right\rceil}-1\right)}{2^{t+1}} > \ln 2$$

$$\frac{\left(2^{\left\lceil \frac{t+1}{2} \right\rceil}-1\right)^2}{2^{t+1}} > \ln 2$$

$$\frac{\left(2^{\frac{t+1}{2}}-1\right)^2}{2^{t+1}} > \ln 2$$

Uvedimo smenu $2^{\frac{t+1}{2}} = \frac{1}{x}$

$$\frac{\left(\frac{1}{x}-1\right)^2}{\frac{1}{x^2}} > \ln 2$$

$$x < 1 - \sqrt{\ln 2}$$

$$-\frac{(t+1)}{2}\ln 2 < \ln(1-\sqrt{\ln 2})$$

$$t > \frac{2}{\ln 2}\left(-\ln\left(1-\sqrt{\ln 2}\right)\right) - 1$$

$$t > 4{,}15647$$ □

Neka je sa $P_h(q)$ obeležena verovatnoća da je rođendanski napad nad heš funkcijom h:D $\rightarrow$ R ostvaren u q pokušaja. Da bi se ostvarila verovatnoća $P_h(q) \geq 0.5$ broj potrebnih pokušaja iznosi $\sqrt{2|R|}$, gde je |R| ukupan broj mogućih heš vrednosti date funkcije h [Taln06]. Da bi se osigurala otpornost heš funkcije na koliziju potrebno je obezbediti preslikavanje poruka u heš vrednosti dužine t-bitova, pri čemu

$$2^{\frac{t+1}{2}} = \sqrt{2|R|}$$

mora biti dovoljno veliko da bi se generisanje $2^{(t+1)/2}$ proizvoljnih poruka i odgovarajućih heš vrednosti smatralo neizvodljivim za napadača. Za heš funkciju h kažemo da je regularna ukoliko se isti broj poruka preslikava u svaku heš vrednost.

Teorema 3:

Neka je heš funkcija *h*: *{0,1}*$^m \rightarrow$ *{0,1}*^{t} regularna i neka je n = $2^{\left\lceil \frac{t+1}{2} \right\rceil}$ za t u intervalu 5 ≤ t < m. Ako su poruke M_1,.....$M_n \in \{0,1\}^m$ slučajno odabrane, tada je

$$1-e^{-\frac{1}{2^{\frac{t+1}{2}}}} < P\text{ [kolizija postoji] } < 1-e^{-\frac{1}{2^{\frac{t+1}{2}}}} + \frac{1}{2^{\frac{t-1}{2}}}$$

Dokaz:

Kako je po pretpostavci heš funkcija *h* regularna, znači da za svaku moguću heš vrednost y $\in$ $\{0,1\}^t$ broj poruka M $\in$ $\{0,1\}^m$, koje zadovoljavaju uslov *h(M)=y*, iznosi 2^{m-t}. Stoga je za svaku heš vrednost y $\in$ $\{0,1\}^t$ i proizvoljnu poruku M

$$P\text{ [}h(M) = y\text{]} = \frac{1}{2^t}$$

Radi jednostavnijeg zapisa, uvodimo smenu 2^t = N.

Neka su M_1,.....M_n nasumično odabrane proizvoljne poruke iz domena $\{0,1\}^m$, i m_1,.....$m_n \in \{0,1\}^t$ odgovarajuće heš vrednosti. Tada se verovatnoća događaja A, da nema kolizije, može zapisati u sledećem obliku:

$$\text{P[nema kolizije]} = \frac{N(N-1)(N-2)....(N-n+1)}{N^n} = \prod_{i=1}^{n-1}(1-\frac{i}{N}) \qquad (1)$$

Primenom nejednakosti

$$1-x < e^{-X} \qquad \text{za } 0 < x < 1$$

dobija se

$$\text{P[nema kolizije]} = \prod_{i=1}^{n-1}(1-\frac{i}{N}) < \prod_{i=1}^{n-1} e^{-\frac{i}{N}} = e^{\sum_{i=1}^{n-1}-\frac{i}{N}} = e^{-\frac{(n-1)n}{2N}}$$

odnosno

$$\text{P[nema kolizije]} < e^{\frac{1}{2^{\frac{t+1}{2}}}-1}$$

Dobijena nejednakost predstavlja gornju granicu verovatnoće događaja A, da nema kolizije, pri čemu je sledeći korak određivanje donje granice.

Dokažimo da je

$$e^{-x} - \frac{x^2}{2} < 1-x \qquad (1.1)$$

Ispitivanjem funkcije $y(x) = e^{-x} - \frac{x^2}{2} + x - 1$ na intervalu $x \in (0,\infty)$, možemo zaključiti da je funkcija definisana na datom intervalu. Kako je prvi izvod funkcije $y'(x) = -e^{-x} - x + 1 < 0$, za $x \in (0,\infty)$ funkcija je strogo opadajuća na datom intervalu. Sledi da je

$$e^{-x} - \frac{x^2}{2} < 1-x$$

Kako je verovatnoća događaja A da nema kolizije

$$\text{P[nema kolizije]} = \prod_{i=1}^{n-1}(1-\frac{i}{N})$$

primenom nejednakosti (1.1) dobijamo

$$P[\text{nema kolizije}] > \prod_{i=1}^{n-1}\left(e^{-\frac{i}{N}} - \frac{i^2}{2N^2}\right)$$

$$> \left(e^{-\frac{1}{N}} - \frac{1}{2N^2}\right)\left(e^{-\frac{2}{N}} - \frac{4}{2N^2}\right)\ldots\left(e^{-\frac{n-1}{N}} - \frac{(n-1)^2}{2N^2}\right)$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{N}} - \sum_{i=1}^{n-1}\left(\frac{i^2}{2N^2} * \prod_{\substack{j=1\\ j\neq i}}^{n-1} e^{-\frac{j}{N}}\right) +$$

$$\sum_{\substack{i,j=1\\ i<j}}^{n-1}\left(\frac{i^2}{2N^2} * \frac{j^2}{2N^2} * \prod_{\substack{k=1\\ k\neq i,j}}^{n-1} e^{-\frac{k}{N}}\right) - \sum_{\substack{i,j,k=1\\ i<j<k}}^{n-1}\left(\frac{i^2}{2N^2} * \frac{j^2}{2N^2} * \frac{k^2}{2N^2} * \prod_{\substack{l=1\\ l\neq i,j,k}}^{n-1} e^{-\frac{l}{N}}\right)$$

+….. +

$$\sum_{i_1<i_2<\ldots<i_x}\left(\frac{i_1^2}{2N^2} * \frac{i_2^2}{2N^2} * \ldots * \frac{i_x^2}{2N^2} * \prod_{k\neq i_1,i_2,\ldots,i_x} e^{-\frac{k}{N}}\right) - \sum_{i_1<i_2<\ldots<j}\left(\frac{i_1^2}{2N^2} * \ldots * \frac{i_x^2}{2N^2} * \frac{j^2}{2N^2} * \prod_{k\neq i_1,i_2,\ldots,i_{x,j}} e^{-\frac{k}{N}}\right)$$

Posmatrajmo treći i četvrti sabirak i dokažimo da je razlika ovih sabiraka veća od 0

$$\sum_{\substack{i,j=1\\ i<j}}^{n-1}\left(\frac{i^2}{2N^2} * \frac{j^2}{2N^2} * \prod_{\substack{l=1\\ l\neq i,j}}^{n-1} e^{-\frac{l}{N}}\right) - \sum_{\substack{i,j,k=1\\ i<j<k}}^{n-1}\left(\frac{i^2}{2N^2} * \frac{j^2}{2N^2} * \frac{k^2}{2N^2} * \prod_{\substack{l=1\\ l\neq i,j,k}}^{n-1} e^{-\frac{l}{N}}\right)$$

$$= \sum_{\substack{i,j=1\\ i<j}}^{n-1}\left(\frac{i^2 j^2}{4N^4} * \prod_{\substack{l=1\\ l\neq i,j}}^{n-1} e^{-\frac{l}{N}}\right) - \sum_{\substack{i,j,k=1\\ i<j<k}}^{n-1}\left(\frac{i^2 j^2 k^2}{4N^4 * 2N^2} * \prod_{\substack{l=1\\ l\neq i,j,k}}^{n-1} e^{-\frac{l}{N}}\right)$$

$$= \sum_{i<j<n-1}\left(\frac{i^2 j^2}{4N^4} * \prod_{l\neq i,j} e^{-\frac{l}{N}}\right) + \sum_{i<j=n-1}\left(\frac{i^2 j^2}{4N^4} * \prod_{l\neq i,j} e^{-\frac{l}{N}}\right) - \sum_{i<j<k}\left(\frac{i^2 j^2 k^2}{4N^4 * 2N^2} * \prod_{l\neq i,j,k} e^{-\frac{l}{N}}\right)$$

$$\geq \sum_{i<j<n-1}\left(\frac{i^2 j^2}{4N^4} * \prod_{l\neq i,j} e^{-\frac{l}{N}}\right) - \sum_{i<j<k}\left(\frac{i^2 j^2 k^2}{4N^4 * 2N^2} * \prod_{l\neq i,j,k} e^{-\frac{l}{N}}\right)$$

$$\geq \sum_{i<j<n-1}\left(\frac{i^2 j^2}{4N^4} * \frac{\prod_{l=1}^{n-1} e^{-\frac{l}{N}}}{e^{-\frac{i}{N}} e^{-\frac{j}{N}}}\right) - \sum_{i<j<k}\left(\frac{i^2 j^2 k^2}{4N^4 * 2N^2} * \frac{\prod_{l=1}^{n-1} e^{-\frac{l}{N}}}{e^{-\frac{i}{N}} e^{-\frac{j}{N}} e^{-\frac{k}{N}}}\right)$$

$$\geq \sum_{i<j<n-1}\left(\frac{i^2 j^2}{4N^4} * e^{\frac{i}{N}} e^{\frac{j}{N}} * \prod_{l=1}^{n-1} e^{-\frac{l}{N}} * \left(1 - \sum_{\substack{k=1 \\ j<k}}^{n-1} \frac{k^2}{2N^2} * e^{\frac{k}{N}}\right)\right)$$

Dokažimo da je suma $\sum_{\substack{k=1 \\ k>j}}^{n-1} \frac{k^2}{2N^2} * e^{\frac{k}{N}} \leq 1$

$$\sum_{\substack{k=1 \\ k>j}}^{n-1} \frac{k^2}{2N^2} * e^{\frac{k}{N}} \leq e^{\frac{n-1}{N}} * \sum_{\substack{k=1 \\ k>j}}^{n-1} \frac{k^2}{2N^2}$$

$$\leq e^{\frac{n-1}{N}} * \sum_{k=1}^{n-1} \frac{k^2}{2N^2}$$

$$\leq \frac{1}{2N^2} * e^{\frac{n-1}{N}} * \sum_{k=1}^{n-1} k^2$$

$$\leq \frac{1}{2N^2} * e^{\frac{n-1}{N}} * \frac{(n-1)n(2n-1)}{6} \qquad (2)$$

Kako je po pretpostavci teoreme $n = 2^{\left\lceil \frac{t+1}{2} \right\rceil}$ i $N=2^t$, grubom procenom nejednakosti (2) dobijamo

$$\leq \frac{1}{2n^4} * e^{\frac{n}{n^2}} * \frac{2n^3}{6}$$

$$\leq \frac{1}{2n^4} * e * \frac{2n^3}{6}$$

$$\leq \frac{e}{n*6}$$

Kako je $\sum_{\substack{k=1 \\ k>j}}^{n-1} \frac{k^2}{2N^2} * e^{\frac{k}{N}} \leq 1$ možemo zaključiti da je razlika trećeg i četvrtog člana

$$\sum_{\substack{i,j=1\\ i<j}}^{n-1}\left(\frac{i^2}{2N^2}*\frac{j^2}{2N^2}*\prod_{\substack{l=1\\ l\neq i,j}}^{n-1}e^{-\frac{l}{N}}\right)-\sum_{\substack{i,j,k=1\\ i<j<k}}^{n-1}\left(\frac{i^2}{2N^2}*\frac{j^2}{2N^2}*\frac{k^2}{2N^2}*\prod_{\substack{l=1\\ l\neq i,j,k}}^{n-1}e^{-\frac{l}{N}}\right)\geq 0$$

Posmatrajmo sada sabirke oblika

$$\sum_{i_1<i_2<\ldots<i_x}\left(\frac{{i_1}^2}{2N^2}*\frac{{i_2}^2}{2N^2}*\ldots*\frac{{i_x}^2}{2N^2}*\prod_{k\neq i_1,i_2,\ldots,i_x}e^{-\frac{k}{N}}\right)-\sum_{i_1<i_2<\ldots<j}\left(\frac{{i_1}^2}{2N^2}*\ldots*\frac{{i_x}^2}{2N^2}*\frac{j^2}{2N^2}*\prod_{k\neq i_1,i_2,\ldots,i_x,j}e^{-\frac{k}{N}}\right)$$

$$=\sum_{i_1<i_2<\ldots<i_x}^{1}\left(\frac{{i_1}^2*{i_2}^2*\ldots*{i_x}^2}{(2N^2)^x}*\prod_{k\neq i_1,i_2,\ldots,i_x}e^{-\frac{k}{N}}\right)-\sum_{i_1<i_2<\ldots<j}\left(\frac{{i_1}^2*{i_2}^2*\ldots*{i_x}^2*j^2}{(2N^2)^x*2N^2}*\prod_{k\neq i_1,i_2,\ldots,i_x,j}e^{-\frac{k}{N}}\right)$$

$$\geq\sum_{i_1<\ldots<i_x<n-1}^{1}\left(\frac{{i_1}^2*\ldots*{i_x}^2}{(2N^2)^x}*e^{\frac{i_1}{N}}*\ldots*e^{\frac{i_x}{N}}\prod_{k=1}^{n-1}e^{-\frac{k}{N}}\right)-\sum_{i_1<\ldots<j}\left(\frac{{i_1}^2*\ldots*{i_x}^2*j^2}{(2N^2)^x*2N^2}*e^{\frac{i_1}{N}}*\ldots*e^{\frac{j}{N}}*\prod_{k=1}^{n-1}e^{-\frac{k}{N}}\right)$$

$$\geq\sum_{i_1<\ldots<i_x<n-1}^{1}\left(\frac{{i_1}^2*\ldots*{i_x}^2}{(2N^2)^x}*e^{\frac{i_1}{N}}*\ldots*e^{\frac{i_x}{N}}\prod_{k=1}^{n-1}e^{-\frac{k}{N}}*\left(1-\sum_{\substack{j=1\\ j>i_x}}^{n-1}\frac{j^2}{2N^2}*e^{\frac{j}{N}}\right)\right)$$

Kako je suma $\sum_{\substack{j=1\\ j>i_x}}^{n-1}\frac{j^2}{2N^2}*e^{\frac{j}{N}}\leq 1$, dokaz je naveden u okviru dokaza za treći i četvrti član, sledi da su razlike članova pozitivne i mogu se zanemariti. Na osnovu dokazanog verovatnoća događaja A, P[nema kolizije], veća je od

$$\text{P[nema kolizije]} > \prod_{i=1}^{n-1}e^{-\frac{i}{N}}-\sum_{i=1}^{n-1}\left(\frac{i^2}{2N^2}*\prod_{\substack{j=1\\ j\neq i}}^{n-1}e^{-\frac{j}{N}}\right)$$

$$> e^{-\frac{1}{N}}e^{-\frac{2}{N}}\ldots.e^{-\frac{n-1}{N}}\left[1-\frac{1}{2N^2}\frac{1}{e^{-\frac{1}{N}}}-\frac{4}{2N^2}\frac{1}{e^{-\frac{2}{N}}}-\ldots.-\frac{(n-1)^2}{2N^2}\frac{1}{e^{-\frac{n-1}{N}}}\right]$$

$$> \prod_{i=1}^{n-1}e^{-\frac{i}{N}}\left[1-\sum_{i=1}^{n-1}\frac{i^2}{2N^2}*\frac{1}{e^{-\frac{i}{N}}}\right]$$

$$> \prod_{i=1}^{n-1}e^{-\frac{i}{N}}-\frac{1}{2N^2}*\prod_{j=1}^{n-1}e^{-\frac{j}{N}}*\sum_{i=1}^{n-1}\frac{i^2}{e^{-\frac{i}{N}}} \qquad (3)$$

Kako je promenljiva $i \leq n-1$ mogu se izvesti sledeće nejednakosti

$$-i^2 \geq -(n-1)^2.$$

odnosno

$$\frac{i}{N} \leq \frac{n-1}{N}$$

$$-e^{\frac{i}{N}} \geq -e^{\frac{n-1}{N}}$$

Primenom dobijenih nejednakosti u nejednakosti (3) sledi:

$$\text{P[nema kolizije]} > \prod_{i=1}^{n-1} e^{-\frac{i}{N}} - \frac{1}{2N^2} * \prod_{j=1}^{n-1} e^{-\frac{j}{N}} * \sum_{i=1}^{n-1} \frac{(n-1)^2}{e^{-\frac{i}{N}}}$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{N}} - \frac{(n-1)^2}{2N^2} * e^{-\frac{(n-1)n}{2N}} * e^{\frac{n-1}{N}} * \sum_{i=1}^{n-1} 1$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{N}} - \frac{(n-1)^3}{2N^2} * e^{\frac{n-1}{N}(1-\frac{n}{2})} \qquad (4)$$

Po pretpostavci teoreme n = $2^{\frac{t+1}{2}}$ i N= 2^t, zamenom u (4) dobija se:

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} - \frac{(2^{\frac{t+1}{2}}-1)^3}{2^{2t+1}} * e^{\frac{2^{\frac{t+1}{2}}-1}{2^t}(1-\frac{2^{\frac{t+1}{2}}}{2})}$$

Kako je $2^{\frac{t+1}{2}} - 1 \leq 2^{\frac{t+1}{2}}$, odnosno, $-(2^{\frac{t+1}{2}} - 1) \geq -2^{\frac{t+1}{2}}$,

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} - \frac{(2^{\frac{t+1}{2}})^3}{2^{2t+1}} e^{\frac{2^{\frac{t+1}{2}}-1}{2^t}(1-\frac{2^{\frac{t+1}{2}}}{2})}$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} - 2^{\frac{1-t}{2}} * e^{2^{\frac{1-t}{2}} - 2^{\frac{1-t}{2}}} * 2^{\frac{t-1}{2}}$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} + \frac{-e^{-1+\frac{1}{2^{\frac{t-1}{2}}}}}{2^{\frac{t-1}{2}}} \qquad (5)$$

Dokažimo da je

$$e^{-1+\frac{1}{2^{\frac{t-1}{2}}}} < 1 + (-1+\frac{1}{2^{\frac{t-1}{2}}}) + (-1 + \frac{1}{2^{\frac{t-1}{2}}})^2$$

$$< \frac{1}{2^{\frac{t-1}{2}}} + 1 - \frac{2}{2^{\frac{t-1}{2}}} + \frac{1}{2^{t-1}}$$

$$< 1- \frac{1}{2^{\frac{t-1}{2}}} + \frac{1}{2^{t-1}}, \text{ odnosno,}$$

$$-e^{-1+\frac{1}{2^{\frac{t-1}{2}}}} > -1+\frac{1}{2^{\frac{t-1}{2}}} - \frac{1}{2^{t-1}}$$

Ispitivanjem funkcije $y(t) = -e^{-1+\frac{1}{2^{\frac{t-1}{2}}}} + 2^{\frac{1-t}{2}} - 2^{1-t} + 1$ na intervalu $x \in (0, \infty)$, možemo zaključiti da je funkcija definisana na datom intervalu. Kako je prvi izvod funkcije $y'(x) = \log(2)\left[\frac{2^{\frac{1-t}{2}}}{2} - 2^{1-t} + \frac{2^{\frac{1-t}{2}}}{2} * e^{-1+2^{\frac{1-t}{2}}}\right] > 0$, za $x \in (0, \infty)$ funkcija je strogo rastuća na datom intervalu, pa je nejednakost

$$-e^{-1+\frac{1}{2^{\frac{t-1}{2}}}} > -1+\frac{1}{2^{\frac{t-1}{2}}} - \frac{1}{2^{t-1}}$$ tačna.

Zamenom u nejednakost (5) dobija se:

$$\text{P[nema kolizije]} > \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} + \frac{1}{2^{\frac{t-1}{2}}} * \left(-1+\frac{1}{2^{\frac{t-1}{2}}} - \frac{1}{2^{t-1}}\right)$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} - \frac{1}{2^{\frac{t-1}{2}}} + \left(\frac{1}{2^{\frac{t-1}{2}}}\right)^2 - \left(\frac{1}{2^{\frac{t-1}{2}}}\right)^3$$

$$> \prod_{i=1}^{n-1} e^{-\frac{i}{2^t}} - \frac{1}{2^{\frac{t-1}{2}}}$$

$$> e^{-\frac{(n-1)n}{2N}} - \frac{1}{2^{\frac{t-1}{2}}}$$

$$> e^{\frac{1}{2^{\frac{t+1}{2}}}-1} - \frac{1}{2^{\frac{t-1}{2}}} \qquad (6)$$

Dobijena nejednakost (6) predstavlja donju granicu verovatnoće događaja A da nema kolizije. Iz dokazanog možemo zaključiti

$$e^{\frac{1}{2^{\frac{t+1}{2}}}-1} - \frac{1}{2^{\frac{t-1}{2}}} < \text{P[nema kolizije]} < e^{\frac{1}{2^{\frac{t+1}{2}}}-1}$$

Na osnovu dobijenih granica verovatnoće događaja A može se izračunati da je verovatnoća komplementarnog događaja B, da kolizija postoji,

$$1- e^{\frac{1}{2^{\frac{t+1}{2}}}-1} < \text{P[kolizija postoji]} < 1- e^{\frac{1}{2^{\frac{t+1}{2}}}-1} + \frac{1}{2^{\frac{t-1}{2}}}$$

što je i trebalo dokazati. □

Dobijeni rezultati iz Teoreme 3, omogućavaju izračunavanje približne vrednosti verovatnoće događaja B, da kolizija postoji. Kako je po pretpostavci Teoreme 3 $n = 2^{\left\lceil \frac{t+1}{2} \right\rceil}$, prilikom izračunavanja približne vrednosti uzimamo da je $n= 2^{\frac{t+1}{2}}$. Kako je vrednost verovatnoće događaja A:

$$\text{P[nema kolizije]} < e^{-\frac{(n-1)n}{2N}}$$

$$< e^{-\frac{2^{t+1}}{2^{t+1}}+\frac{2^{\frac{t+1}{2}}}{2^{t+1}}}$$

$$< e^{-1} * e^{\frac{1}{2^{\frac{t+1}{2}}}}$$

Po pretpostavci teoreme t ≥ 5, sledi da je

$$\text{P[nema kolizije]} < e^{-\frac{7}{8}}$$

Sa povećanjem vrednosti promenljive t razlomak $\frac{1}{2^{\frac{t+1}{2}}} \to 0$, a vrednost verovatnoće događaja A

$$\text{P[nema kolizije]} \leq e^{-1} = 0.368$$

Slično se u slučaju donje granice, za verovatnoću događaja A pod uslovom pretpostavke teoreme da je t ≥ 5 može izračunati

$$\text{P[nema kolizije]} > e^{-1} * e^{\frac{1}{2^{\frac{t+1}{2}}} - \frac{1}{2^{\frac{t}{2}}}} = 0.119$$

Kako razlomci $\frac{1}{2^{\frac{t+1}{2}}}$ i $\frac{1}{2^{\frac{t-1}{2}}} \to 0$ sa porastom vrednosti promenljive t, može se zaključiti da verovatnoća događaja A

$$\text{P[nema kolizije]} \geq 0.368$$

Na osnovu rezultata vrednosti gornje i donje granice verovatnoće događaja A dobijamo da je P[nema kolizije] ~ 0.368, dok je verovatnoća komplementarnog događaja B, da kolizija postoji, sa povećanjem vrednosti promenljive t

$$\text{P[kolizija postoji]} \sim 0.632, \text{ za } t \geq 19$$

U Tabeli 4. date su vrednosti verovatnoće događaja B.

t	$1-e^{-\frac{1}{2^{\frac{t+1}{2}}}}$
5	0.583
6	0.598
7	0.608
8	0.615
9	0.620
10	0.624
11	0.626
12	0.628
13	0.629
14	0.630
15	0.631
16	0.631
17	0.631
18	0.632
19	0.632
20	0.632
21	0.632
22	0.632
23	0.632
24	0.632
25	0.632

Tabela 4. Verovatnoće događaja B za različite vrednosti promenljive t

Zaključak:

Dobijeni rezultati potvrđuju da postoji značajna korelacija između sigurnosti heš funkcije i broja generisanih poruka, odnosno, da se otpornost heš funkcije na rođendanski napad obezbeđuje nemogućnošću generisanja $2^{\frac{t+1}{2}}$ poruka i odgovarajućih heš vrednosti dužine t-bitova. U suprotnom, vrednost verovatnoće događaja B da kolizija postoji u slučaju rođendanskog napada veća je od 0,5 za n= $2^{\frac{t+1}{2}}$ pokušaja i njena približna vrednost iznosi 0.632.

Teorema 4:

Ako regularna heš funkcija h preslikava $h:\{0,1\}^m \rightarrow \{0,1\}^t$, za t u intervalu $3 \leq t < m$, pri čemu je $n = 2^{\left\lfloor \frac{t-k}{2} \right\rfloor}$, i poruke $M_1,.....M_n \in \{0,1\}^m$ slučajno odabrane, tada je

$$P\text{ [kolizija postoji]} < \frac{1}{2^{k+1}}$$

Dokaz:

Kako je heš funkcija regularna, tada za svako $y \in \{0,1\}^t$, važi $|h^{-1}(y)| = 2^{m-t}$. Neka je B_i događaj da i-ta poruka M_i ima istu heš vrednost kao neka od prethodnih poruka. Tada je

$$P[B_i] \leq \frac{i-1}{2^t}$$

$$P[\text{kolizija postoji}] = P[B_1 \cup B_2 \cup \ldots\ldots \cup B_n]$$

$$\leq \sum_{i=2}^{n} P[B_i]$$

$$\leq \sum_{i=2}^{n} \frac{i-1}{2^t}$$

$$\leq \frac{n(n-1)}{2^{t+1}}$$

$$< \frac{n^2}{2^{t+1}} \leq \frac{2^{t-k}}{2^{t+1}} = \frac{1}{2^{k+1}} \quad \square$$

7. Osetljivost digitalnog potpisa

Dosadašnja istraživanja koja se odnose na rođendanski napad i uslove potrebne za ostvarenje kolizije, polaze od pretpostavke da je heš funkcija h regularna, pri čemu se u svaku heš vrednost preslikava približno isti broj poruka. Iako su heš funkcije i njihova primena u oblasti digitalnog potpisa poznate javnosti već duži niz godina, u literaturi je opisan relativno mali broj trivijalnih primera koji se odnose na neregularne heš funkcije i više su od teorijskog nego od praktičnog značaja.

Stinson u [Stin95], navodi da je Teorema 3. tačna pod pretpostavkom da je h regularna funkcija. Buhman (*eng. Buchmann*) u svojoj diskusiji rođendanskog napada [Buch00] naglašava da ditribucija nad odgovarajućim heš vrednostima mora biti uniformna. Stinson kasnije navodi [Stin06] da se otpornost na koliziju povećava pod određenim uslovima, a jedan od njih je da je heš funkcija regularna.

Navedeni dokazi i pretpostavke oslanjaju se na regularnost heš funkcije pri čemu se ne navode nikakve indikacije o slučaju kada heš funkcija h nije regularna niti o broju potrebnih pokušaja za ostvarenje kolizije u tom slučaju. Bellar (*eng. Bellare*) u [Bell04] nameće pitanje da li je pod ovim okolnostima broj pokušaja potrebnih za postizanje kolizije značajno manji od $\sqrt{2 \mid R \mid}$?

Osnovna zamisao ovog rada jeste da analiza napada ne zavisi od algoritma heš funkcije. Cilj istraživanja jeste da dobijeni rezultati važe za svaku heš funkciju, a ne samo za specifično odabrane.

Konstrukcija neregularnih heš funkcija predstavlja prvi korak u testiranju osetljivosti digitalnog potpisa na rođendanski napad, pri čemu se neregularnost ostvaruje narušavanjem uniformne raspodele heš funkcija. Bez obzira na to što do sada poznati napadi na regularne heš funkcije ne pružaju željene odgovore kada su neregularne heš funkcije u pitanju, svaki od njih daje novi uvid u principe dizajniranja neregularnih heš funkcija i stimuliše dalja istraživanja u ovoj oblasti.

Praktičnim ispitivanjem lako se pokazuje da sa porastom neregularnosti heš funkcije raste i brzina uspeha rođendanskog napada. Intuitivno posmatrano navedeno tvrđenje ne predstavlja iznenađujuću činjenicu. U ekstremnom slučaju može se posmatrati heš funkcija kojom se sve poruke M_i preslikavaju u istu heš vrednost m. Opšte je poznato da je u navedenom slučaju verovatnoća uspeha rođendanskog napada, odnosno postizanja kolizije:

P[kolizija postoji] = 1

U daljem nastavku, kroz detaljnu obradu nekoliko primera, posebna pažnja biće usmerena na proučavanje osetljivosti heš funkcija na rođendanski napad u slučaju kada su heš funkcije neregularne. Dok je u radu [Bell04] obrađen samo trivijalan primer preslikavanja svih poruka u istu heš vrednost, u ovom radu obratićemo pažnju na slučajeve koji se mogu smatrati predstavnicima određenih grupa primera.

Podela je izvršena u odnosu na činjenicu da li su verovatnoće preslikavanja svih heš vrednosti različite ili se samo jedna od njih razlikuje od ostalih. Zatim su u slučaju pojedinačnog izdvajanja obrađeni primeri kada je verovatnoća preslikavanja jednaka konstanti koja ne zavisi od t, i kada je verovatnoća preslikavanja jednaka promenljivoj koja zavisi od t. Na osnovu ovakve podele definisani su sledeći primeri:

- primer neregularne heš funkcije kod koje je verovatnoća preslikavanja jedne heš vrednosti jednaka konstanti koja ne zavisi od promenljive t
- primer neregularne heš funkcije kod koje je verovatnoća preslikavanja jedne heš vrednosti jednaka promenljivoj koja zavisi od promenljive t
- primer neregularne heš funkcije kod koje su verovatnoće preslikavanja heš vrednosti međusobno različite

Lema 2. Bernulijeva nejednakost: Za svaki prirodan broj n i svaki realan broj x, takav da je x ≥ -1 važi $(1+x)^n \geq 1+nx$

Dokaz: Matematičkom indukcijom lako se dokazuje da je

za n=0, B(0): $(1+x)^0 \geq 1+0x$, odnosno 1≥1

za n=1, B(1): $(1+x)^1 \geq 1+1x$, odnosno $1+x \geq 1+x$

Pretpostavimo da nejdnakost vazi za n, B(n): $(1+x)^n \geq 1+nx$, treba dokazati da važi

B(n+1): $(1+x)^{n+1} \geq 1+(n+1)x$

$$(1+x)^{n+1} = (1+x)(1+x)^n$$

$$\geq (1+x)(1+nx) \text{ jer važi B(n)}$$

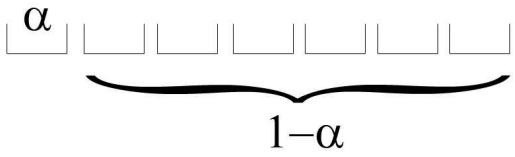
$$\geq 1+(n+1)x+nx^2$$

$$\geq 1+(n+1)x \qquad \square$$

7.1 Primer neregularne heš funkcije sa verovatnoćom preslikavanja jednakoj konstanti za jednu heš vrednost

Neka heš funkcija h preslikava *h*: $\{0,1\}^m \rightarrow \{0,1\}^t$, pri čemu je $N = 2^t$ ukupan broj heš vrednosti. Pretpostavimo da samo za jednu od heš vrednosti važi da je verovatnoća preslikavanja proizvoljne poruke M_i u naznačenu heš vrednost m* jednaka konstanti α. Iz skupa svih poruka $\{0,1\}^m$ posmatramo n slučajno izbabranih proporuka $M_1,.....,M_n$ koje se preslikavaju u različite heš vrednosti $m_1,....,m_n$. Verovatnoća da se proizvoljna poruka M_i preslika u m* iznosi α, dok je verovatnoća da se poruka M_i ne preslika u m* jednaka $1-\alpha$. Možemo razlikovati dva slučaja:

1. Slučaj I - kada se svih n poruka preslika u n različitih heš vrednosti, pri čemu ni jedna od heš vrednosti nije m* sa verovatnoćom α. Verovatnoća ovog slučaja može se zapisati kao $P_I \leq (1-\alpha)^n$
2. Slučaj II – kada se jedna od n poruka preslika u m* čija je verovatnoća α. Verovatnoća ovog slučaja može se zapisati kao $P_{II} \leq n\alpha\,(1-\alpha)^{n-1}$



Slika 9. Raspodela verovatnoća neregularne heš funkcije

Tada je ukupna verovatnoća događaja A:

$$\begin{aligned} P[\text{nema kolizije}] &\leq (1-\alpha)^n + n\alpha\,(1-\alpha)^{n-1} \\ &\leq (1-\alpha)^{n-1}\,((1-\alpha)+ n\alpha) \\ &\leq (1-\alpha)^{n-1}\,(1+ \alpha(n-1)) \end{aligned}$$

Primenom Bernulijeve nejednakosti

$$\begin{aligned} &\leq (1-\alpha)^{n-1}\,(1+ \alpha)^{n-1} \\ &\leq (1-\alpha^2)^{n-1} \end{aligned}$$

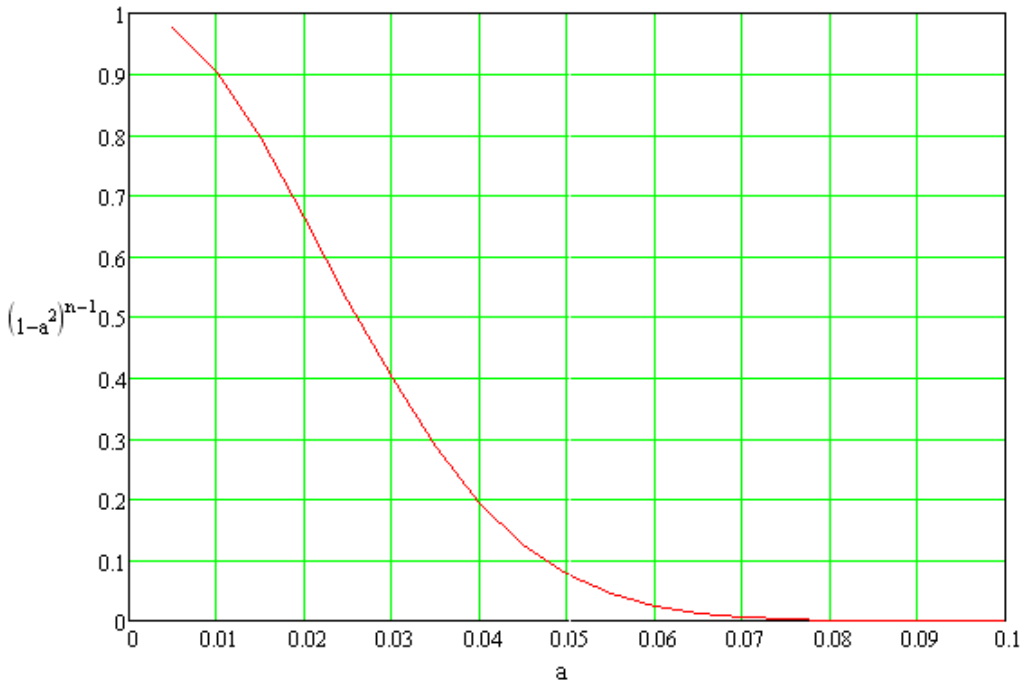
Kada konstanta $\alpha \rightarrow 1$, verovatnoća događaja A, $(1-\alpha^2)^{n-1} \rightarrow 0$, čime verovatnoća komplementarnog događaja B, da kolizija postoji,

$$P[\text{kolizija postoji}] \rightarrow 1.$$

U Tabeli 5. dat je prikaz promene vrednosti verovatnoće događaja A u slučaju kada konstanta α uzima vrednosti iz intervala $\alpha \in$ [0.005, 0.01], uz pretpostavku da je t=20. Grafikon funkcije $f(\alpha)=(1-\alpha^2)^{n-1}$ u slučaju navedenih vrednosti prikazan je na Slici 11.

α	$f(\alpha)=(1-\alpha^2)^{n-1}$
0.005	0.975
0.010	0.903
0.015	0.794
0.020	0.664
0.025	0.528
0.030	0.398
0.035	0.285
0.040	0.194
0.045	0.126
0.050	0.077
0.055	0.045
0.060	0.025
0.065	0.013
0.070	0.007
0.075	0.003
0.080	0.001
0.085	0.001
0.090	0.001
0.095	0.001
0.100	0.001

Tabela 5. Prikaz promene vrednosti verovatnoće događaja A u slučaju različitih vrednosti konstante α



Slika 10. Prikaz promene vrednosti verovatnoće događaja A u slučaju različitih vrednosti konstante α

Zaključak:

Dobijeni rezultat potvrđuje da se sa povećanjem neregularnosti heš funkcije povećava uspešnost kolizionog napada, odnosno, da je verovatnoća događaja A, da nema kolizije, najveća u slučaju kada je heš funkcija regularna, odnosno kada se isti broj poruka preslikava u svaku heš vrednost, a da se sa povećanjem vrednosti konstante α i narušavanjem regularnosti heš funkcije povećava i uspešnost kolizionog napada.

7.2 Primer neregularne heš funkcije kod koje jedna heš vrednost ima verovatnoću preslikavanja veću od ostalih

Neka heš funkcija h preslikava *h*: $\{0,1\}^m \rightarrow \{0,1\}^t$, pri čemu je $N = 2^t$ ukupan broj heš vrednosti. Pretpostavimo da samo za jednu od heš vrednosti važi da je verovatnoća preslikavanja proizvoljne poruke M_i u naznačenu heš vrednost m* veća od ostalih i obeležimo je sa α, dok ostale heš vrednosti imaju istu vrednost verovatnoće preslikavanja obeleženu sa β. Iz skupa svih poruka $\{0,1\}^m$ posmatramo n slučajno izbabranih poruka M_1,.....,M_n koje se preslikavaju u različite heš vrednosti m_1,....,m_n. Možemo razlikovati dva slučaja:

1. Slučaj I - kada se n poruka preslikava u n različitih heš vrednosti, pri čemu sve heš vrednosti imaju istu verovatnoću β. Verovatnoća ovog slučaja može se zapisati kao

$$P_I=(N-1)(N-2)(N-3)*.....*(N-n)\ \beta^n$$

2. Slučaj II – kada se jedna poruka preslikava u m*, dok se preostalih n-1 poruka preslikava u heš vrednosti čija je verovatnoća β. Verovatnoća ovog slučaja može se zapisati kao

$$P_{II}=n\alpha\ (N-1)(N-2)(N-3)*.....*(N-n+1)\ \beta^{n-1}$$

U slučaju kada regularna heš funkcija h preslikava *h*: $\{0,1\}^m \rightarrow \{0,1\}^t$, sve heš vrednosti imaju istu verovatnoću preslikavanja koja iznosi $\frac{1}{N}$, pri čemu je $N = 2^t$. U ovom primeru regularnost heš funkcije narušena je povećanjem verovatnoće preslikavanje jedne heš vrednosti u odnosu na ostale. Iz navedenog se može pretpostaviti da je

$$\beta = \frac{1}{N} - x,$$

$$\alpha = \frac{1}{N} + (N-1)x$$

odakle sledi da je

$$x = \frac{1}{N} - \beta$$

$$x < \frac{1}{N}$$

Ukupna verovatnoća događaja A da nema kolizije predstavlja zbir verovatnoća P_I i P_{II}, odnosno:

P[nema kolizije] $= (N-1)(N-2)*.....*(N-n)\ \beta^n + n\alpha\ (N-1)(N-2)(N-3)*.....*(N-n+1)\ \beta^{n-1}$

$= (N-1)(N-2)*.....*(N-n+1)\ \frac{(1-Nx)^{n-1}}{N^{n-1}}\ [N\beta + n(\alpha-\beta)]$

$= \frac{(N-1)(N-2)*.....*(N-n+1)}{N^{n-1}}\ (1-Nx)^{n-1}[N\beta + n(\alpha-\beta)]$

U Teoremi 3 u slučaju uniformne raspodele, verovatnoća događaja A, da kolizija ne postoji, zapisana je u obliku:

$$P^U_{[\text{nema kolizije}]} = \frac{(N-1)(N-2)....(N-n+1)}{N^{n-1}}$$

odakle sledi da je

$P[\text{nema kolizije}] = P^U_{[\text{nema kolizije}]} * (1-Nx)^{n-1}[N\beta + n(\alpha-\beta)]$

$= P^U_{[\text{nema kolizije}]} * (1-Nx)^{n-1}[1-Nx+n(\frac{1}{N} +(N-1)x-\frac{1}{N} +x)]$

$= P^U_{[\text{nema kolizije}]} * (1-Nx)^{n-1}[1+ (n-1)\ Nx]$

Primenom Bernulijeve nejednakosti dobija se

$(1-Nx)^{n-1}[1+ (n-1)\ Nx] \leq (1-Nx)^{n-1}(1+ Nx)^{n-1}$

$\leq (1-N^2x^2)^{n-1}$

Kako je $(1-N^2x^2)^{n-1} < 1$sledi da je

$P[\text{nema kolizije}] < P^U_{[\text{nema kolizije}]}$

odnosno važi da je verovatnoća komplementarnog događaja B, da kolizija postoji,

$P[\text{kolizija postoji}] > P^U_{[\text{kolizija postoji}]}$

Zaključak:

Dosadašnjom matematičkom analizom, čiji su dokazi prethodno navedeni, dokazano je da je verovatnoća događaja B, da kolizija postoji, veća u slučaju neregularne raspodele heš funkcije.

7.3 Primer neregularne heš funkcije sa različitim verovatnoćama preslikavanja

Neka heš funkcija h preslikava *h*: *{0,1}*$^m \rightarrow$ *{0,1}*^{t}, pri čemu je N = 2^t ukupan broj heš vrednosti. Pretpostavimo da je verovatnoća preslikavanja proizvoljne poruke M_i različita za svaku heš vrednost, pri čemu važi da je zbir verovatnoća $p_1+p_2+....+p_N$ =1 i pi ≥ 0 za 1 ≤ i ≤ N. Iz skupa svih poruka $\{0,1\}^m$ posmatramo n slučajno izbabranih poruka $M_1,.....,M_n$ koje se preslikavaju u različite heš vrednosti $m_1,....,m_n$. Pokažimo da je verovatnoća događaja A, da nema kolizije, manja u slučaju neuniformne raspodele, odnosno:

$$\sum_{i_1,..i_n} p_{i_1} p_{i_2}.....p_{i_n} \leq \begin{pmatrix} N \\ n \end{pmatrix} \frac{n!}{N^n}$$

pri čemu je $1 \leq i_j \leq N$, za $1 \leq j \leq n$, dok su i_1, i_2,..i_n međusobno različiti.

Verovatnoću događaja A, da nema kolizije, prilikom uniformne raspodele možemo svesti na zapis:

$$P^U_{[\text{nema kolizije}]} = \frac{N(N-1)(N-2)....(N-n+1)}{N^n} = \begin{pmatrix} N \\ n \end{pmatrix} \frac{n!}{N^n}$$

Neka je sa $L = \sum_{i_1,..i_n} p_{i_1} p_{i_2}.....p_{i_n}$ označena suma verovatnoća. L možemo posmatrati kao funkcija od $p_1,.....,p_n$, odnosno, $L=L(p_1,.....,p_n)$ jer $i_j \in \{1.2……N\}$. Funkcija $L(p_1...p_n)$ predstavlja neprekidnu funkciju, polinom, N promenljivih, definisanu na kompaktnom skupu D: $p_1 \geq 0$, $p_2 \geq 0...p_N \geq 0$, $p_1+p_2+....+p_N =1$. D je kompaktan skup jer je ograničen, zatvoren skup R^N. Funkcija L dostiže apsolutni maksimum na skupu D, a pri tome je $L(p_1,.p_i..p_j..,p_n) \leq L(p_1,.(p_i+p_j)/2,p_{i+1,...} (p_i+p_j)/2.. p_{j+1,...},p_n)$. Za proizvoljne $i,j \in \{1,2,….,N\}$, pri čemu je i≠j mogu se izdvojiti sledeći sabirci:

1. Sabirci u kojima figurišu oba broja p_i, p_j.
2. Sabirci u kojima figuriše jedan od brojeva p_i ili p_j
3. Preostali sabirci koji ne sadrže niti p_i niti p_j

Kako je $p_i * p_j \leq (\frac{p_i + p_j}{2})^2$ sledi da je

$$\sum_{i_1,..i_n} p_1 p_2 ... p_i p_{i+1} ..... p_j p_{j+1} ..... p_n \leq \sum_{i_1,..i_n} p_1 p_2 ... \frac{p_i + p_j}{2} p_{i+1} ..... \frac{p_i + p_j}{2} p_{j+1} ..... p_n$$

U slučaju kada u sabirku figuriše jedan od brojeva p_i ili p_j sabirci se mogu grupisati u parove, pri čemu se zbir takvih sabiraka neće promeniti ukoliko umesto p_i ili p_j stavimo $\frac{p_i + p_j}{2}$.

Funkcija L ne dostiže maksimum ako svi $p_1, p_2, ..., p_N$ nisu međusobno jednaki, odnosno ukoliko ne važi da je $p_1 = p_2 = ... = p_N = \frac{1}{N}$. Kako je broj sabiraka jednak $\binom{N}{n} n!$, a vrednost svakog od sabiraka u datom slučaju jednaka $\frac{1}{N^n}$, proizilazi da je

$$\sum_{i_1,..i_n} p_{i_1} p_{i_2} ..... p_{i_n} \leq \binom{N}{n} \frac{n!}{N^n}$$

pri čemu se jednakost ostvaruje samo u slučaju kada je $p_1 = p_2 = ... = p_N = \frac{1}{N}$, odnosno, kada je u pitanju uniformna raspodela. Iz navedenog sledi da je

$$P_{[\text{nema kolizije}]} \leq P^U_{[\text{nema kolizije}]}$$

Zaključak:

Navedenom matematičkom analizom dokazano je da je verovatnoća događaja B, da kolizija postoji, u slučaju neregularne heš funkcije veća u odnosu na regularnu heš funkciju.

7.4. Balans heš funkcija

Jedno od najvažnijih svojstava heš funkcije, kada je digitalni potpis u pitanju, jeste otpornost na koliziju, odnosno, da je za zadato P nemoguće izračunati P' takvo da je h(P) = h(P'). Iz navedenih primera u Poglavljima 7.1, 7.2 i 7.3 može se zaključiti da je verovatnoća postizanja kolizije veća u slučaju neregularnih heš funkcija. Pitanje koje se nameće jeste da li se može izračunati "količina regularnosti" heš funkcije.

Belar i Kono (*eng. Bellar, Kohno*) u svom radu [Bell04], definišu meru *balans heš funkcije*. Ova mera predstavlja realan broj $\mu(h) \in [0,1]$ pri čemu je heš funkcija h regularna samo u slučaju kada je vrednost $\mu(h)=1$. Ukoliko je vrednost balansa heš funkcije $\mu(h) \neq 1$ funkcija je neregularna, a neregularnost se povećava kako se balans $\mu(h)$ približava 0. Belar i Kono definišu balans na sledeći način:

Definicija 11.

Neka je h heš funkcija koja preslikava $h:D \rightarrow R$, pri čemu je D domen, $R=\{R_1,....,R_r\}$, $d=|D|$ i $r=|R|$. Obeležimo sa $d_i = |h^{-1}(R_i)|$ broj svih poruka $m \in D$ koje se preslikavaju u heš vrednost R_i, za datu funkciju h, odnosno, $h(m) = R_i$. Balans heš funkcije h obeležavamo $\mu(h)$ i definišemo

$$\mu(h) = \log_r \left[\frac{d^2}{d_1^2 + ... + d_r^2} \right] \qquad (*)$$

gde $\log_r(.)$ predstavlja logaritam za osnovu r.

Tvrđenje:

Ako je h heš funkcija, tada je $0 \leq \mu(h) \leq 1$, pri čemu je $\mu(h)=1$ ako je h regularna funkcija, a $\mu(h)=0$ u slučaju kada je h konstantna funkcija.

Dokaz:

Datu jednakost (*) možemo zapisati u obliku $\frac{1}{r^{\mu(h)}} = \frac{d_1^2 + ... + d_r^2}{d^2}$.

Neka je

$$S = \{(x_1,\ldots,x_r) \in R^r : x_1 + ... + x_r = d\}.$$

Definišimo funkciju $f: S \rightarrow R$ tako da je

$$f(x_1,\ldots,x_r) = x_1^2 + ... + x_r^2 \text{ za proizvoljno } x_1,\ldots,x_r \in S$$

Neka je

$\text{Min}_S(f) = \min \{ f(x_1,\ldots,x_r) : (x_1,\ldots,x_r) \in S \}$
$\text{Max}_S(f) = \max \{ f(x_1,\ldots,x_r) : (x_1,\ldots,x_r) \in S \}$

Primenom definicije balansa heš funkcije možemo zaključiti da je

$$\text{Min}_S(f) \le \frac{d^2}{r^{\mu(h)}} \le \text{Max}_S(f)$$

Funkcija *f* dostiže minimum na skupu S kada je $d_i = \frac{d}{r}$ za svako $i \in \{1,...,r\}$ iz čega proizilazi da je $\text{Min}_S(f) = \frac{d^2}{r}$ što odgovara zaključku da je funkcija h regularna, odnosno, da se isti broj poruka, $\frac{d}{r}$, preslikava u svaku heš vrednost. Sa druge strane funkcija *f* dostiže maksimum kada je $\begin{cases} x_i = d \\ x_j = 0,\ j \neq i \end{cases}$ iz čega sledi da je $\text{Max}_S(f) = d^2$ što odgovara zaključku da je funkcija h konstantna funkcija. Iz navedenog sledi da je

$\frac{d^2}{r} \le \frac{d^2}{r^{\mu(h)}} \le d^2$, odnosno $1 \le r^{\mu(h)} \le r$,

primenom logaritma za osnovu r dobijamo $0 \le \mu(h) \le 1$. □

U Poglavlju 7.2. analizom primera neregularne heš funkcije kod koje jedna heš vrednost ima verovatnoću preslikavanja veću od ostalih identifikovan je odnos verovatnoća u slučaju uniformne i neuniformne raspodele:

$$\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}} = \left(1 - Nx\right)^{n-1}\left(1 - Nx + nNx\right)$$

Kako vrednost promenljive x zavisi od N i n, može se uvesti smena $nNx = a$,

$$\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}} = \left(1 - \frac{a}{n}\right)^{n-1}\left(1 - \frac{a}{n} + a\right)$$

$$= \left(1 + \frac{1}{-\frac{n}{a}}\right)^{(-\frac{n}{a})\frac{n-1}{n}(-a)}\left(1 - \frac{a}{n} + a\right)$$

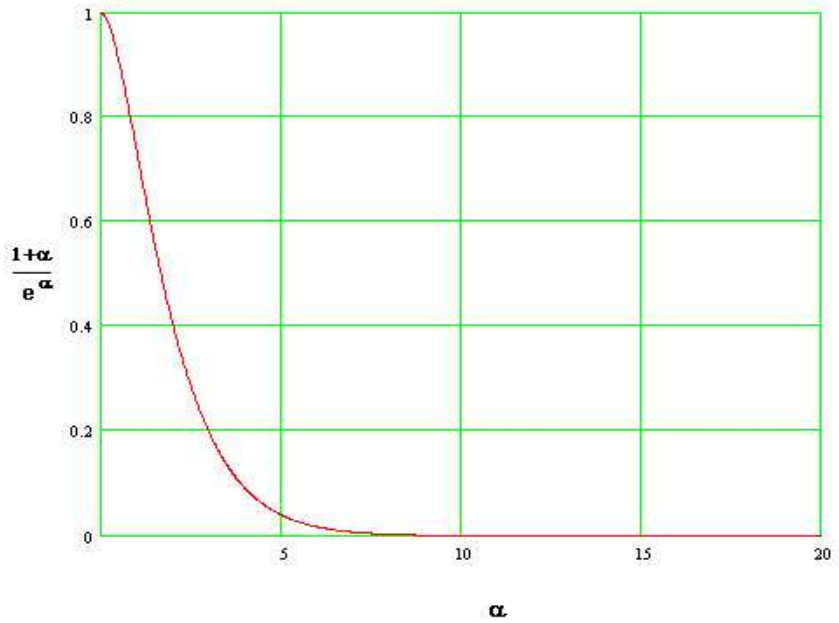
U slučaju kada n $\to \infty$ razlomak $\frac{n-1}{n} \to 1$, dok razlomak $\frac{a}{n} \to 0$. Kako je

$$e = \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n$$

odnos verovatnoća dobija oblik:

$$\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}} = \frac{1+a}{e^{a}}$$

Ispitivanjem funkcije $y(a) = \frac{1+a}{e^{a}}$ možemo zaključiti da je funkcija definisana na intervalu [0,+∞) i da ne dostiže nultu tačku u datom intervalu definisanosti. Kako je prvi izvod funkcije $y'(a) < 0$, za svako $a \in [0,\infty)$ funkcija je strogo opadajuća, a maksimum dostiže u tački $a = 0$. Kako je $\lim_{a\to\infty} y(a) = 0$, funkcija $y(a)$ ima horizontalnu asimptotu y=0. Kombinacijom prethodno navedenih rezultata dobija se grafikon funkcije koji je prikazan na Slici 11.



Slika 11. Grafički prikaz odnosa verovatnoća u slučaju uniformne i neuniformne raspodele

U skladu sa dobijenim rezultatima sledi da se odnos verovatnoća $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}}$ može posmatrati kao realan broj iz intervala [0,1]. Maksimalna vrednost

ostvaruje se u slučaju kada je $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}} = 1$, odnosno, kada je heš funkcija regularna, pri čemu verovatnoća preslikavanja iznosi $\frac{1}{N}$ za svaku heš vrednost. Minimalna vrednost dostiže se u slučaju kada je $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}} = 0$, odnosno, kada je heš funkcija konstantna funkcija.

Dobijeni rezultati o odnosu verovatnoća postizanja kolizije u slučaju regularnih i neregularnih heš funkcija podudaraju se sa Tvrđenjem u istraživanju Belara i Kona. Analitičkim određivanjem odnosa $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}}$ date heš funkcije, određuje se balans heš funkcije, a na taj način i brzina uspeha rođendanskog napada.

8. Zaključak

Heš funkcije i njihova primena u okviru digitalnog potpisa predstavljaju relativno noviju oblast kriptografije. U poređenju sa brojem primera kolizionih napada na regularne heš funkcije, za napade na neregularne heš funkcije moglo bi se reći da je njihovo prisustvo u literaturi vrlo oskudno. Upravo ovo je bio motiv da se pristupi intenzivnijem proučavanju neregularnih heš funkcija. Činjenica da u literaturi postoji relativno mali broj kriptoanalitičkih metoda namenjenih napadu na neregularne heš funkcje, otvara prostor za formulisanje i istraživanje novih tehnika i postupaka koji bi bacili više svetla na osobine neregularnih heš funkcija.

U ovom radu je posebno obrađen rođendanski napad kao najčešći kolizioni napad koji spada u grupu napada grubom silom eng.(*Brute force attack)*. Analiza ovog napada sprovedena je nad neregularnim heš funkcijama, i to u obliku generalnog pristupa kriptoanalizi neregularnih heš funkcija. Generalnim pristupom omogućeno je istraživanje opštih karakteristika neregularnih heš funkcija i njihovih slabosti pod rođendanskim napadom.

Na osnovu analize različitih predstavnika heš funkcija sa neuniformnom raspodelom, koji su obrađeni u ovom radu, dobijeni su rezultati koji potvrđuju slabosti i nedostatke neregularnih heš funkcija u odnosu na regularne funkcije. Bolji rezultati, odnosno veća otpornost na koliziju, ostvareni su svaki put u korist regularnih heš funkcija. Analizom navedenih primera neregularnih heš funkcija dokazana je uspešnost rođendanskog napada sa povećanjem neuniformnosti heš funkcije. Obradom dobijenih informacija identifikovan je pojam “količina regularnosti” odnosno, balans heš funkcije.

Mera balans heš funkcije određuje se preko odnosa verovatnoća otpornosti na koliziju u slučaju uniformne i neuniformne raspodele $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}}$ i predstavlja realan broj iz intervala [0,1]. Ekstremne vrednosti 0 i 1 ostvaruju se u slučaju kada je heš funkcija konstantna funkcija, $\mu(h) = 0$, dok se vrednost $\mu(h) = 1$ ostvaruje kada je funkcija regularna. Proučavanje odnosa $\frac{P_{[\ nemakolizije\ ]}}{P^{U}_{[\ nemakolizije\ ]}}$ predstavlja samo jedan od kriterijuma koji je potrebno uzeti u obzir prilikom kreiranja heš funkcije, ali se ne može smatrati i dovoljnim za postizanje otpornost heš funkcije na rođendanski napad.

Buduća istraživanja mogu se odvijati u više pravaca pri čemu bi jedan od značajnih smerova predstavljalo utvrđivanje dodatnih kriterijuma potrebnih za preciznije izračunavanje balansa heš funkcija, čime bi se omogućilo otkrivanje brzine uspeha rođendanskog napada na datu heš funkciju. Jedan od važnih koraka ovog istraživanja jeste provera da li poznati heš algoritmi čuvaju balans komprimujućih funkcija, odnosno, da li se dizajniranjem komprimujućih funkcija visokog balansa osigurava i visok balans heš funkcije.

Literatura

[Abda00] Abdalla M., Reyzin L., A New Forward-Secure Digital Signature Scheme, Advances in Cryptology - Asiacrypt 2000, Springer Berlin, 2000.

[Baig06] Baigneres T., Junod P., Yi Lu, Monnerat J., Vaudenay S., A classical introduction to cryptography exercise book, Springer Science+Business Media, Inc., 2006.

[Bell04] Bellare, M., Kohno, T., Hash function balance and its impact on the birthday attack, Advances in Cryptology EURPCRYPT 2004, Springer, 2004

[Buch00] Buchmann J., Introduction to cryptography, Springer, 2000

[Chut89] Chute, A; Balthazar, L; Poston, C: Learning from Teletraining, Pennsylvania State University, 1989

[Diff76] Diffie W., Hellman M., New Directions in Cryptography, http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

[Ecry06] ECRYPT Yearly Report on Algorithms and Keysizes, 2006, http://www.ecrypt.eu.org/

[Hale06] Halevi S., Krawczyk, H., Strengthening Digital Signatures via Randomized Hashing, Advances in Cryptology - Crypto 2006, Springer, 2006.

[Inte06] The Intelligent Edu, Computer Security for Everyone, 2006. http://www.intelligentedu.com/computer_security_for_everyone/introduction-to-computer-security.html

[Kahn67] Kahn D., ”The Codebreakers”, The Macmillan Company, New York, 1967.

[Kels05] Kelsey J., Schneier, B., Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work, Advances in Cryptology - Eurocrypt 2005, Springer Berlin, 2005.

[Knud94] Knudsen Lars, Block Ciphers - Analysis, Design and Applications, http://www.daimi.au.dk/PB/485/PB-485.pdf,1994.

[Leht06] Lehtinen, R., Computer Security Basics, 2nd Edition, O'Reilly, 2006.

[Mene96] Menezes A., van Oorschot P., Vanstone S., “Handbook of Applied Cryptography”, CRC Press, 1996.

[Oppl05] Oppliger R., Contemporary Cryptography, Artech House Computer Security Library, 2005.

[Pete98] Peterson, I. "MathTrek: Birthday Surprises." 1998 http://www.maa.org/mathland/mathtrek_11_23_98.html

[Rodr06] Rodriguez, H.D.; Aguirre, O.,Interoperability and Reusability of Knowledge in a Constructivist Web-Based Learning CSCL System Electronics, Robotics and Automotive Mechanics Conference, 2006

[Riel05] Riele, H., Factoring large numbers tests security of electronic data transport, 2005 http://www.cwi.nl/research/2005/24teRieleEs.pdf

[Schn96] Schneier B., Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, John Wiley & Sons, Inc, 1996.

[Sloa07] The Sloan Consortium, Five Years of Growth in Online Learning, 2007 http://www.sloan-c.org/publications/survey/survey07.asp

[Stei96] Steiner, V. What is distance education, 1996. http://www.wested.org/tie/dlrn/distance.html

[Stin95] Stinson D., Cryptography: Theory and Practice, CRC Press, 1995.

[Stin06] Stinson D., Some observations on the theory of cryptographic hash functions, Designs, Codes and Cryptography, Springer, 2006.

[Taln06] Talnor J., Welsh D. Complexity and Cryptography an Introduction, Cambridge University Press, 2006.

[Tane04] Tanenbaum A., Računarske mreže prevod četvrtog izdanja, Mikro knjiga, 2005.

[Weip05] Weippl E., Security in E-Learning, Vienna University of Technology, Springer Science+Business Media, Inc, 2005.

.