FBIM Transactions
DOI 10.12709/fbim.04.04.01.03

IZBOR METODE KRIPTOVANJA PODATAKA U BEŽIČNIM RAČUNARSKIM MREŽAMA

THE CHOISE OF METHOD OF DATA ENCRYPTION IN WIRELESS COMPUTER NETWORKS

Tamara Cvetković
Fakultet za poslovno industrijski menadžment, „Union – Nikola Tesla“
Univerzitet u Beogradu, Beograd, Srbija

Milan Mihajlović
Fakultet za poslovno industrijski menadžment, „Union – Nikola Tesla“
Univerzitet u Beogradu, Beograd, Srbija

Živanka Miladinović
Fakultet za poslovno industrijski menadžment, „Union – Nikola Tesla“
Univerzitet u Beogradu, Beograd, Srbija

Jel kategorija: **D85**

Apstrakt

U doba sve veće popularnosti bežičnih lokalnih računarskih mreža (WLAN) i sve izraženije potrebe da se njihovim korišćenjem omogući mobilnost korisnika unutar prostora pokrivenog signalom WLAN-a, neophodno je obezbediti jednostavnost njihove upotrebe uz istovremenu zaštitu informacija koje cirkulišu ovim mrežama. Dovoljno pouzdana zaštita može se postići izborom odgovarajućeg metoda enkripcije. Kriptogrami, šifrovane informacije se mogu prenositi LAN mrežom i Internetom uz minimum opasnosti da budu kompromitovane. U ovom radu je posebna pažnja posvećena bežičnim mrežama, jer su one i najizloženije rizicima, zbog raznovrsnosti korisnika i uređaja kojima treba obezbediti pristup. Posle uvodnog dela u kome su razmotreni neki kriptografski algoritmi i metodi javnog i tajnog ključa, u radu su detaljnije razmotreni neki mogući napadi i njihov uticaj na bezbednost podataka, kao i mogućnosti zaštite informacija tokom njihovog prenosa i mirovanja, uz analizu rizika primene kriptografije. U završnom delu rada dati su zaključci dobijeni na osnovu izvršenih analiza.

Adresa autora zaduženog za korespodenciju:
Tamara Cvetković
tamara-cvetkovic@live.com

Ključne reči: *bežične, mreže, šifrovanje, ključ, algoritam, bezbednost*

Abstract

In the era of the increasing popularity of wireless local area networks (WLAN) and the increasing need to facilitate their use user mobility within the area covered by the WLAN signal, it is necessary to ensure their ease of use while protecting the information that is circulating these networks. Just reliable protection can be achieved by selecting the appropriate method of encryption. Cryptograms, encrypted information can be transmitted by the LAN and the Internet with a minimum risk of being compromised. In this paper special attention to wireless networks, because they are the most exposed to risks, due to the diversity of users and devices that access should be ensured. After the introductory part in which they discussed some cryptographic algorithms and methods of public and secret key, the paper further discussed some of the possible attacks and their impact on data security, as well as opportunities to protect information during its transmission and standstill, with the risk analysis of the application of cryptography. The final part provides conclusions obtained on the basis of the analyses.

Keywords*: wireless, networks, encryption, key, algorithm, safety*

1 BEŽIČNE MREŽE I TEHNOLOGIJE ZAŠTITE PODATAKA

U bežičnim računarskim mrežama postoje rizici vezani za sigurnost podataka. Rizici u elektronskom poslovanju podrazumevaju rizike u poslovnoj komunikaciji putem Intereneta, gde podaci u poslovnim porukama mogu biti kompromitovani ili razotkriveni, i rizike vezane za računarski sistem, odnosno interni računarski sistem preduzeća, kada informacije dolaze spolja, sa Interneta. (Bjelić, 2012)

Sa razvojem računarskih mreža kriptografija sve više dobija na značaju, jer je bitno na neki način se zaštititi i obezbediti važne podatke koji se prenose putem mreže. Šifriranje prenosnih paketa obezbeđuje postizanje poverljivosti i bezbednosti.

Šifrovanjem podataka se štite informacije od spoljnog sveta, tako da niko, osim primaoca, ne može da zna koja informacija se šalje. (Claude, Einar, Gene, & Refik, 2010) Informacije se štite na različite načine. U *end-to-end* enkripciji ni jedan čvor ne sme da ima uvid u sadržaj primljenih podataka. Koristeći ovaj pristup moguće je garantovati da će biti teže za prisluškivača da dobije pristup podacima. Drugi način rešavanja problema prisluškivanja je korišćenje *globalnog ključa* za šifrovanje ili samo ključeva između susednih čvorova, ali u tom slučaju je end-to-end enkripcija izgubljena. Za prvi pristup, koji ima jedan globalni ključ, prisluškivač bi mogao dobiti pristup svim informacijama samo hakovanjem jednog čvora i određivanjem globalnog ključa. (Claude, Einar, Gene, & Refik, 2010)

Zaštita podataka se preduzima sa namerom sprečavanja štetnih posledica njihove zloupotrebe. (Bjelić, 2012, str. 212) Jako je važno znati kako zaštititi podatke u poslovnoj komunikaciji, odnosno onemogućiti osobama kojima nisu namenjene poruke, tj. koje nisu primaoci, da steknu uvid u poslate poruke. Na taj način podaci ostaju poznati samo pošiljaocu i primaocu i oni ih jedino mogu koristiti. Glavna opasnost je mogućnost zloupotrebe ovih podataka.

Podaci koji se mogu zloupotrebiti podrazumevaju javne podatke, tj. podatke u koje svi imaju uvid; podatke zaštićene autorskim pravom, odnosno podatke u koje svi imaju uvid ali su zaštićeni autorskim pravom; poverljive podatke, koji su tajni ali njihovo postojanje nije tajno; i tajne podatke kod kojih je i njihovo postojanje tajna. Predmet zaštite moraju biti samo poverljivi i tajni podaci. Ako se podaci razmenjuju nekim komunikacionim kanalom onda se primenjuju tehnike šifrovanja podataka pre puštanja u komunikacionu mrežu, odnosno kriptografske tehnike zaštite podataka. (Bjelić, 2012)

2 KRIPTOGRAFSKI ALGORITMI I METODI JAVNOG I TAJNOG KLJUČA

Kriptografijom se podaci transformišu iz izvornog u šifrovani ili kriptografski oblik pre slanja, a kada ih primi drugi subjekt ti podaci se iz šifrovanog oblika vraćaju u izvorni oblik. U prevodu kriptografija znači pisanje tajni i ona uključuje enkripciju odnosno šifrovanje poruka, i dekripciju tj. dešifrovanje poruka. (Bjelić, 2012, str. 213,214)

Kriptografija uključuje više disciplina, i povezana je sa matematikom, a u poslednje vreme i sa informatikom i računarstvom. U kriptografiji se koristi matematička funkcija (algoritam) i koriste se unapred utvrđena pravila odnosno ključevi da bi se kreirala kriptovana poruka, a kasnije i dešifrovala i omogućava se čuvanje važnih podataka i njihov prenos preko računarske ili telekomunikacione mreže, a da se ne vrše zloupotrebe od strane neovlašćenih korisnika. Na taj način se obezbeđuju i štite podaci od zloupotreba i osigurava se da ni jedan korisnik kome poruka nije namenjena ne može da vidi koji je sadržaj poruke. Ukoliko sadržaj kriptovanog teksta saznaju neovlašćeni korisnici oni ipak ne mogu pročitati izvorni tekst.

Uz pomoć kriptografskog algoritma se obavlja šifrovanje izvornog teksta. Svaki kriptografski algoritam za ulazne podatke koristi izvorni tekst i ključ, a rezultat je kriptovani tekst. Dešifrovanjem se omogućava da se od kriptovanog teksta dobije originalni izvorni tekst, odnosno vrši se suprotni postupak od kriptovanja. Kriptogram je kriptovani tekst za koji nije poznat ključ.

Kriptografija obuhvata metode očuvanja tajnosti informacija. Ona mora da obezbedi integritet ili verodostojnost informacija koje se šifruju čime se vodi računa o tome da ne dođe do nedozvoljene promene informacija, što može uključiti promenu informacije, njeno brisanje ili zamenu. Da bi se obezbedila istinitost informacije, mora se na neki način proveriti da li je informacija promenjena od strane neovlašćene osobe; tajnost informacija obezbeđuje da je sadržaj informacije dostupan samo ovlašćenim osobama odnosno samo onima koji poseduju ključ. Pored toga, mora sadržati i proveru identiteta kada korisnici koji počinju komunikaciju vrše predstavljanje jedan drugome a onda počinju sa razmenom informacija; nemogućnost izbegavanja odgovornosti što je veoma bitno, naročito u novije vreme kada se veliki deo novčanih transakcija obavlja putem Interneta.

Šifrovani podaci su zaštićeni od neovlašćenog pristupa, s obzirom da korisnik koji ne poseduje ključ nema pristup šifrovanim podacima. Algoritam za šifrovanje se može smatrati sigurnim ukoliko sigurnost šifrata zavisi samo od tajnosti ključa, ali ne i od tajnosti algoritma. (Pleskonjić, Maček, Đorđević, & Carić, 2007) Dužina ključa ili broj simbola koji predstavljaju ključ, zavisi od kriptografskog algoritma. Pored zaštite otvorenog teksta neophodno je zaštititi i ključ.

I dalje ne postoji algoritam koji u potpunosti osigurava od nelegalnog dobijanja poruke preko šifrata. Ukoliko je dobar algoritm, onda je potrebno da cena razbijanja šifrata bude veća od vrednosti informacije zbog koje se to radi, kao i da vreme potrebno za to bude dovoljno dugo, tako da dobijena informacija postane neupotrebljiva i zastarela. (Cvijetić, Avram, & Bratić, 2008) Veoma je važan način upotrebe algoritma i njegove primene kako bi se obezbedila što veća sigurnost enkriptovanih podataka.

U novije vreme, kriptografske metode podrazumevaju postojanje *kriptografskih algoritama,* koji transformišu podatke, odnosno vrše njihovo šifrovanje i dešifrovanje. Kriptografski algoritmi uključuju skup pravila po kojima se vrši kriptovanje. Algoritmi za kriptovanje su tajni algoritmi u kojima se bezbednost zasniva na tajnosti algoritma i algoritmi zasnovani na ključu u kojima se bezbednost zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati. Ovde je algoritam javno poznat, a ključ se čuva u tajnosti. S obzirom da je ključ niz podataka koji se koristi za kriptovanje drugih podataka, mora se koristiti i za dekriptovanje podataka.

Algoritam koji obavlja šifrovanje i dešifrovanje, odnosno *sistem šifra*, može sadržati jednu ili više metoda koji uključuju metod zamene/ substitucije, metod transpozicije i metod algebre. Pri supstituciji šifara karakteri otvorene tekst poruke su zamenjeni karakterima drugog pisma ili numeričke vrednosti. Originalni karakteri u šifratu gube svoj identitet, ali zadržavaju svoje pozicije. U transpoziciji šifra karakteri iz otvorenog teksta su preuređeni u njihovom redosledu. Iako originalni karakteri gube pozicije, oni zadržavaju svoj identitet. Algebratske šifre mogu da se zasnivaju na veoma složenoj metodi transpozicije ili uključiti metodu supstitucije, ili čak upotrebi obe metode zajedno sa matematičkom transformacijom koja se obavlja uz pomoć računara. Sa dolaskom računara, složene algebarske šifre su se brzo razvile. (Harold & FICS, 1997)

Danas se, dakle, koriste tri opšte kategorije kriptografskih algoritama:

- *simetrični (metod jedinstvenog – privatnog ključa),* koji podrazumeva korišćenje samo jednog ključa i za šifrovanje, i za dešifrovanje poruke koja je bila šifrovana, s tim da tim ključem rapolažu samo pošiljalac i primalac podataka;
- *asimetrični (metod javnog ključa*) koji podrazumeva korišćenje dva ključa u kriptografskom procesu, jednog za kreiranje kriptovane poruke, a drugog za njeno dešifrovanje, s tim da su ključevi matematički povezani; *i*
- *hashing algoritmi*. Svaki od kriptografskih algoritama ima svoje jače strane i svoje mane. Ponekad se kombinuju ovi algoritmi kako bi se iskoristile njihove prednosti. Takvom kombinacijom sistema kriptografije nastaju hibridni sistemi.

Simetrični kriptografski algoritmi koriste isti ključ i za kodiranje i za dekodiranje podataka. Kod simetričnih algoritama ključevi moraju biti sakriveni ili tajni. Ukoliko ključ otkriju strane koje nisu uključene u komunikaciju, postoji velika opasnost po sigurnost podataka koja može biti i potpuno eliminisana. To podrazumeva da svako ko poseduje tajni ključ može da čita i piše šifrovane poruke. Učesnici u komunikaciji dele tajni ključ i moraju da štite pristup ključu.

Javni ključ je poznat osobama s kojima korisnik želi da komunicira, dok je privatni ili tajni ključ poznat samo korisniku koji je ovlašćen da dešifruje poruke. Privatni i javni ključ su matematički povezani, ali se privatni ključ ne može odrediti na osnovu javnog ključa. (Pleskonjić, Maček, Đorđević, & Carić, 2007) Kod ove metode može nastati problem prenosa tajnog ključa, jer ukoliko se tajni ključ presretne, poruka može da se pročita. To je razlog upotrebe ovog tipa enkripcije najčešće prilikom zaštite podataka koji se ne dele sa drugima. Prednost ovih algoritama jeste brzina, pa se oni i koriste kada postoji potreba za dosta čitanja i pisanja u baze podataka. Dužina ključa je jako važna za sigurnost podataka.

Moguće je izvršiti više napada na podatke šifrovane simetričnim algoritmom. Moguć je i napad poznat kao „nagađanje i provera“ i obično je uspešan kada se algoritam primenjuje na osnovu loše proizvoljno izabranog ključa. Ovde napadač nagađa koji je ključ upotrebljen za šifrovanje, a zatim pokušava primeniti ključ da proveri da li je taj ključ odgovarajući.

Moguć je takođe i napad na kriptografski sistem grubom silom i zasniva se na proveravanju svih mogućih ključeva. Kako je rasla snaga računara koja je omogućila kreiranje i proveru brojnih ključeva za relativno kratak period vremena, ovi napadi su postajali uspešniji. Ukoliko se koriste baze podataka sa simetričnim algoritmom, u tom slučaju je preporučena minimalna dužina ključa od 128-bita i sve ispod toga dovodi podatke u nepotreban rizik. (Cvijetić, Avram, & Bratić, 2008)

Kod simetričnih kriptosistema ili kriptosistema sa tajnim ključem se za kriptovanje/dekriptovanje poruka koristi isti ključ. Jedna osoba ima za cilj slanje poruke drugoj osobi preko nezaštićenog komunikacionog kanala. Osoba koja šalje poruku najpre generiše poruku koja se upućuje u blok za šifrovanje, u kome se vrši kriptovanje poruke uz korišćenje ključa dobijenog uz pomoć generatora ključa. Na taj način se kreira kriptovana poruka. Potom se tako dobijena poruka komunikacionim kanalom šalje do primaoca.

Simetrične šifre rade tako što blokovski otvoreni tekst podele u blokove i koriste specijalno konstruisane funkcije koje određenim operacijama pomešaju blok otvorenog teksta sa ključem čime se dobija šifrovani tekst. Da bi se izbegao napad korišćenjem rečnika, koriste se blokovi velikih dužina (64, 128 i više bitova). Ideja se sastoji u aproksimaciji slučajne permutacije na velikom skupu ulaza. Koristi se i metoda višestrukih transformacija. Osnovne metode koje se koriste su metode supstitucije i permutacije. (Markagić & Markagić, 2013)

Postupak dekriptovanja se obavlja inverznim postupkom od kriptovanja u bloku za dekriptovanje. Obe strane moraju držati ključ u tajnosti, odnosno ključ se ne sme prenositi nezaštićenim komunikacionim kanalom. Za razliku od ključa, kriptovana poruka može da se šalje i po nezaštićenom kanalu s obzirom na to da sadržaj izvorne poruke može da protumači samo onaj korisnik koji ima ključ.

Za razliku od algoritama sa tajnim ključem gde se koristi jedan deljeni ključ, *asimetrični algoritmi* koriste dva ključa, pri čemu je jedan od ključeva javni, a drugi privatni. Najpre se generiše javni ključ na osnovu tajnog ključa koji zadaje primalac. Javni ključ se daje strani koja šalje šifrovane podatke primaocu. Uz pomoć javnog ključa, pošiljalac šifruje podatak koji šalje i takav podatak šalje primaocu. Kad šifrat stigne, primalac dešifruje podatak uz pomoć svog tajnog ključa. Dakle, tajni ključ ima samo primalac, a javni ključ može imati bilo ko, pošto se on koristi samo za šifrovanje, a ne i za dešifrovanje. Prednost ovog načina šifrovanja je u tome što nema opasnosti ukoliko neko presretne javni ključ, jer pomoću njega mogu samo da se šifruju podaci. Brzina nije prednost asimetričnih operacija, i mnogo su sporije nego operacije kod simetričnih algoritama, tako da nisu odgovarajuće za strategije enkripcije baza podataka, jer mogu imati veliki uticaj na performanse baze podataka. Asimetrični algoritmi su se pokazali kao spori ukoliko se polja često dešifruju u realnom vremenu, a ukoliko se podaci pišu jednom i nakon toga retko koriste,onda se mogu koristiti asimetrični algoritmi. (Cvijetić, Avram, & Bratić, 2008) Najpoznatiji algoritmi s javnim ključem su RSA i ElGamal. (Pleskonjić, Maček, Đorđević, & Carić, 2007, str. 57)

Razlika između simetričnih i asimetričnih algoritama je u tome što simetrični algoritmi koriste isti ključ za kriptovanje i dekriptovanje, dok asimetrični algoritmi koriste različite ključeve za kriptovanje odnosno dekriptovanje. Informacije koje su kriptovane javnim ključem mogu se dekriptovati samo tajnim ključem odnosno to može uraditi samo osoba koja je vlasnik tajnog asimetričnog ključa. Oba ključa moraju biti povezana pomoću jedinstvene jednosmerne funkcije, odnosno ne sme se izračunati tajni ključ iz javnog ključa ili se barem ne sme izračunati u razumnom vremenu.

S obzirom da simetrična i asimetrična kriptografija imaju prethodno pomenute nedostatake, poput problema prenosa tajnog ključa kod simetričnih algoritama ili sporosti asimetričnih operacija, javlja se potreba za sistemima koji kombinuju najbolje pojedinačne karakteristike oba sistema. S tom potrebom su nastali *hibridni kriptosistemi.* Ovaj sistem funkcioniše tako što se prvo izvorni tekst kriptuje upotrebom ključa, a zatim se taj ključ zajedno sa kriptovanom porukom pakuje i ponovo kriptuje javnim ključem osobe kojoj se šalje poruka. Postupak dekripcije je obrnut, odnosno osoba koja je primila poruku je prvo dekriptuje svojim tajnim ključem, pronalazi zapakovani *session* ključ i koristi ga da bi pročitala izvornu poruku.

Jedna od kriptografskih tehnika, koja pokazuje da li je poruka primljena u transportu, je *hash funkcija* koja podrazumeva matematički proces, zasnovan na algoritmu, kojim se poruka sažima u hash rezultat. Kada primalac primi poruku, on primećuje ovu funkciju. Ako je poruka neovlašćeno izmenjena, on će dobiti drugačiju hash vrednost od one koju mu je pošiljalac doznačio uz poruku. Hash funkcije spadaju u kriptografske algoritme bez ključa. *Hash funkcija* kompresuje niz podataka proizvoljne dužine u niz podataka fiksne dužine. Heš funkcije se koriste kod zaštite integriteta podataka. Dakle, kada stigne novi podatak upotrebljava se hash funkcija i vrši se poređenje sa hash vrijednosti originala i ukoliko podaci nisu korumpirani ili izmenjeni vrednosti će biti identične, a ukoliko su podaci bili izmenjeni, hash vrednosti će biti različite. Hashing algoritmi ne koriste ključ i kod njih dužina ključa nije problem. Hashing nije reverzibilan proces tako da nema ni opasnosti od dešifrovanja. (Cvijetić, Avram, & Bratić, 2008)

Heš funkcija pretvara ulazni podatak promenljive dužine u izlazni podatak fiksne dužine- heš i njima se utvrđuje integritet poruke. Heš se može posmatrati kao otisak prsta- prilikom slanja poruke, pošiljalac šalje i heš poruke. Na osnovu otiska, primalac može odrediti da li je poruka koju je primio stigla u originalnom ili izmenjenom obliku. Heš funkcijom se beskonačan skup poruka preslikava se u konačan skup heš vrednosti. Kod jednoparametarskih heš funkcija, ulazni argument je samo poruka, a kod dvoparametarskih to je poruka i javni ključ. (Pleskonjić, Maček, Đorđević, & Carić, 2007, str. 107)

Kombinovanjem metode privatnog ključa i hash funkcije dobija se nova metoda zaštite podataka- *elektronski (digitalni) potpis*, na osnovu kog se može identifikovati pošiljalac i dokazati verodostojnost poruke. (Pleskonjić, Maček, Đorđević, & Carić, 2007) Kada se na originalnu poruku primeni hash funkcija dobija se hash

vrednost. Na tu vrednost se primenjuje metod privatnog ključa kako bi vrednost bila poznata samo pošiljaocu i primaocu. Ono što se dobija je digitalni potpis koji se koristi za proveru poruke. Pošto kombinuje dve tehnike, digitalni potpis se koristi i za proveru intregriteta poruke (izmenjenosti) i za zaštitu podataka, ali on služi i za potvrdu porekla poruke. (Bjelić, 2012, str. 213-214)

Većina zemalja je danas i pravno uredila oblast elektronskog potpisa jer je ona izuzetno značajna za razvoj elektronskog poslovanja. Elektronski potpis danas ima snagu pravog potpisa i validan je pri zaključenju ugovora i izdavanje poslovne dokumentacije za označavanje originalnih dokumenata. Danas se elektronski dokumenti priznaju sa istom pravnom snagom kao i papirnati dokumenti, zahvaljujući postojanju elektronskog potpisa. (Bjelić, 2012, str. 213-214)

Različite vrste enkripcije se primenjuju u zaštiti sistema baza podataka u odnosu na podatke koji se kriptuju i na nivou na kojem se kriptovanje obavlja: enkripcija za zaštitu podataka tokom prenosa; tokom mirovanja; enkripcija na nivou aplikacije; na nivou baze podataka; enkripcija fajla i transparentna enkripcija.

Prema alatima koji se koriste, enkripcija može biti softverska i hardverska, pri čemu se softverska upotrebljava da označi proces kriptovanja podataka u samom procesoru, a ukoliko se podaci šifruju pomoću hardvera priključenih na računar onda je u pitanju hardverska enkripcija. Hardverska enkripcija je brža u odnosu na softversku enkripciju, ali ona može biti nedostupna, pa se onda koristi softverska enkripcija. (Cvijetić, Avram, & Bratić, 2008)

3 NAPADI I BEZBEDNOST PODATAKA

Bezbednost je veoma bitna u virtuelnim privatnim mrežama i treba se zaštititi od velikog broja napada u mreži, i to napada autentifikacije, kriptografskih napada, napada integriteta, falsifikovanja servera, falsifikovanja paketa, napada uskraćivanja usluga i pasivnog monitorovanja. (Mašović, Saračević, & Zornić, 2011) Cilj napada na šifrat je otkrivanje otvorenog teksta ili ključa kojim je šifrovan otvoreni tekst.

Prekidanje, presretanje, modifikacija i izmišljanje su osnovne *pretnje po bezbednosti informacije.* U pasivnom napadu na bezbednost se samo prisluškuje poruka i on se teže otkrva od aktivnog napada. U aktivnom napadu dolazi do menjanja poruke, maskiranja i/ili ponovnog slanja modifikovane poruke. (Markagić & Markagić, 2013)

Moguće su različite vrste napada na šifarski sistem, odnosno mogućnosti dolaženja do sadržaja ključa i otvorenog teksta (Markagić & Markagić, 2013) Primer za to je napad poznatim šifrovanim tekstom, što je najteža vrsta napada kada kriptoanalitičar poznaje samo algoritam šifrovanja i poseduje kriptogram odnosno šifrovani tekst. Tada kriptoanalitičar ima samo šiftrate nekoliko poruka šifrovanih pomoću istog algoritma. On treba da otkrije otvoreni tekst što većeg broja poruka ili ako je moguće da otkrije ključ kojim su poruke šifrovane. Napad može uključiti i napad poznatim otvorenim tekstom, kada za određeni šifrovani tekst kriptoanalitičar poznaje otvoreni tekst ili jedan njegov deo i poznaje algoritam i poseduje određeni broj otvorenih i šifrovanih tekstova, ali ne poznaje ključ; napad odabranim otvorenim tekstom kada kriptoanalitičar sam određuje neki otvoreni tekst i šifruje ga i poznaje algoritam, šifrovani tekst i određeni broj parova otvorenih i šifrovanih tekstova, ali ne zna ključ. Ostale vrste napada mogu uključiti:

- napad odabranim šifrovanim tekstom, kada kriptoanalitičar ima privremeni pristup alatu za šifrovanje tako da može dobiti šifrat odabranog otvorenog teksta;
- napad odabranim šifratom, kada kriptoanalitičar koristi napad odabranim otvorenim tekstom, a rezultati napada se koriste za odabir nekog drugog otvorenog teksta, ovaj napad poznat je i pod nazivom „diferencijalna kriptoanaliza", kriptoanalitičaru je poznat algoritam, šifrovani tekst, odabrani otvoreni tekst sa šifrovani tekstom i odabrani šifrovani tekst sa otvorenim tekstom; (Poljak, 2006)
- potkupljivanje, ucena i krađa ne spadaju u matematičke oblike kriptoanalize, ali se često primenjuju (Pleskonjić, Maček, Đorđević, & Carić, 2007, str. 58);

- „birthday attack“ – ovaj napad je dobio ime po paradoksu rođendana;
- „meet in the middle“ – sličan Birthday napadu, osim što kriptoanalitičar može proveriti presek između dva skupa, a ne mora čekati pojavljivanje vrednosti dvaput u jednom skupu;
- napad korišćenjem srodnih ključeva – kod ovog napada pretpostavlja se znanje o odnosu između ključeva u dva različita šifrovanja i ovaj napad može otkriti slabosti u postupku generisanja podključeva;
- delimično znanje o ključu – napadač poseduje delimično znanje o tajnom ključu. (Markagić & Markagić, 2013)

Postupci kriptoanalize podrazumevaju klasičnu kriptoanalizu (frekvencijska analiza, kasiski ispitivanje) simetrične algoritme (diferencijalna kriptoanaliza, linearna kriptoanaliza, mod-n kriptoanaliza, XSL napad) i ostale metode (Birthday attack, Meet in the Middle, DeCSS, Gardening). (Markagić & Markagić, 2013)

4 ZAŠTITA PODATAKA TOKOM PRENOSA I MIROVANJA

Prilikom prenošenja podatka od baze do primaoca i obrnuto podaci se mogu obezbediti metodama kriptovanja i mogu se obezbediti isto tako i tokom mirovanja. Podaci se mogu prenosti lokalnom mrežom, putem Interneta ili preko bežičnih mreža. Kako bi se sprečilo otkrivanje sadržaja poruke neophodna je enkripcija podataka. *Data-at-rest* podrazumeva sve podatke koji su u okviru sistema baza podataka, a koji se ne prenose kroz mrežu ili podatke koji se samo trenutno zadržavaju u memoriji dok čekaju da se izvrši nihovo čitanje ili ažuriranje.

Enkripcija podataka koji miruju ili *data at rest* je šifrovanje podataka koji se čuvaju u sistemima baza podataka. Najčešće se koriste:

- *enkripcija na nivou aplikacije* (ova enkripcija omogućava da se podaci šifruju i kao takvi smeštaju u baze podataka). Ukoliko je korektna i ispravna primena ove vrsta enkripcije podaci su onda zaštićeni od napada na storage, krađe storage media i napada od zlonamernih administratora baza podataka. Međutim moguće je u ovoj enkripciji doći do korištenja podataka samo kroz aplikaciju. Ovo ne mora biti nedostatak, jer se na taj način možda može sprečiti napad od strane zlonamernih administratora. Negativna strana ove enkripcije jeste to što se dešifovanje vrši na strani klijenta i zato hakeri koji kompromituju klijentske aplikacije imaju pristup dešifrovanim podacima).
- *Enkripcija na nivou baze podataka* omogućava da se obezbede podaci dok se upisuju ili čitaju iz baze podataka. Negativna strana upotrebe ovog pristupa to što su podaci u formi otvorenog teksta između aplikacije i baze podataka i to može dovesti do opterećenja performansi. Ovim pristupom se postiže transparentnost u odnosu na aplikaciju, kratko je vreme primene, podaci su enkriptovani na disku ili mediju za backup podataka, i troškovi održavanja su minimalni.
- *Enkripcija na nivou fajla,* odnosno *na nivou zapisa*, štiti osetljive podatke u fajlovima baza podataka od svih napadača koji nemaju ključ za enkriptovanje. Enkripcijom na nivou fajla se obezbeđuje zaštita podataka od napada sa nivoa operativnog sistema i smanjuje se rizik od fizičkih napada, dosta je jednostavna primena ove metode i kratko je vreme primene, i lako se održava. Loša strana ovog metoda je što se ne može sprečiti napadi na nivou baze podataka. Nedostatak ovog pristupa je i to što se ne može se kriptovati pojedinačni deo fajla već samo ceo fajl. (Cvijetić, Avram, & Bratić, 2008)
- *Transparentna enkripcija* se automatski primenjuje pri svakoj promeni ili unosu potencijalno osetljivih podataka. Automatskom primenom enkripcije nestaje potreba za eksplicitnim pozivanjima enkripcijskih funkcija, i naj način se mogu sprečiti neke programske greške. Transparentna enkripcija podrazumeva i to da je ona transparentna samo autorizovanim korisnicima, ali ne napadačima. (Cvijetić, Avram, & Bratić, 2008)

Pretraživanje celog prostora je najjednostavnija i najsporija vrsta napada. Napadač vrši dekriptovanje šifrovanog teksta sa svim mogućim ključevima koji se mogu pojaviti. Imajući u vidu da

je algoritam šifrovanja javno dostupan, ovaj napad nije moguće sprečiti. Napadač kod ovog napada ima poznat otvoreni tekst ili otvoreni tekst ima neku poznatu strukturu. (Poljak, 2006)

Pretraživanje pola prostora je metoda primenjiva na šifre koje pokazuju određeno svojstvo simetričnosti i smanjuje vreme napada za polovinu. Ovaj napad koristi se ako je poznat par otvorenog i kriptovanog teksta za koje važi svojstvo komplementa. Za poslednji bit ključa postavi se vrednost '0' i pretražuje prostor sa preostalim delom ključa. Ako se za neki ključ dobije šifrovani tekst, zaključuje se da je taj ključ pravi ključ. Ako se dobije komplement otvorenog teksta, zaključuje se da je pravi ključ komplement od primenjenog. (Poljak, 2006)

5 UPRAVLJANJE KLJUČEVIMA I RIZICI PRIMENE KRIPTOGRAFIJE

Primena kriptografije unosi i određene rizike. Postoji rizik od gubitka ili brisanja ključa, usled čega može doći do gubitka podataka koji su njime šifrovani. Celokupna sigurnost može biti narušena na taj način. Ključ se može upotrebiti za dekriptovanje podataka. Upravljanje ključevima podrazumeva predlog rešenja kako da se pristupi ključevima, kako upravljati ključevima, gde su locirani, kako se može napraviti rezervna kopija, i kako se oni mogu oporaviti, kako se kontroliše njihova upotreba i beleži pristup. Hardware Security Modul (HSM) omogućava zaštitu ključeva od svih pretnji, a ukoliko HSM ne postoji onda se oni trebaju čuvati odvojeno od baze podataka. (Cvijetić, Avram, & Bratić, 2008)

Ključ mora biti zaista slučajan. Ne generše se algoritmima koji kao ulaz koriste kraći ključ. Mora biti bez biasa: verovatnoća svih simbola mora biti jednaka. Ključ mora biti jednake dužine kao i poruka. Znakovi u poruci i ključu moraju biti iz iste abecede jednake veličine. Ključ se na poruku mora primeniti tako da su za date simbole otvorenog teksta, svi simboli kriptovanog teksta jednako mogući i obratno. Osim za kriptovanje poruke, ključ nema drugu namenu. Drugi način zaštite je kontinuirana promena ključa. Za probijanje šifre sa javnim ključem, bezbednost leži u teškoći računanja tajnog ključa uz poznavanje javnog ključa. Dakle, samo se *one-time pad* može smatrati sigurnom šifrom.

6 ZAKLJUČAK

Enkripcija je postala neophodna u savremenom poslovanju, kada postoji veliki rizik od gubitka podataka i svakodnevne krađe. Šifrovanje se može koristiti i koristi se pri čuvanju podataka na hard diskovima računara. Pristup uskladištenim fajlovima se može ograničiti primenom lozinki. Međutim, uprkos činjenici da su uskladišteni podaci ugroženiji od neovlašćenih upotreba i krađa nego podaci koji se prenose, enkripcijom se ipak najviše štite podaci koji se prenose. Sistemi za enkcipciju pomažu da se popuni rastući bezbednosni gep u bežičnoj komunikaciji, i na taj način se obezbeđuju podaci i sprečavaju njihove zloupotrebe od strane neovlašćenih lica.

CITIRANI RADOVI

Bjelić, P. (2012). *Globalna elektronska trgovina.* Beograd: Ekonomski fakultet Univerziteta u Beogradu.

Claude, C., Einar, M., Gene, T., & Refik, H. (2010). Efficient Aggregation of encrypted data in Wireless Sensor Networks. *Lehrstuhl für Rechnernetze und Telematik Seminar*, 4.

Cvijetić, B., Avram, D., & Bratić, M. (2008). Use cryptography for security database. *INFOTEH-JAHORINA Vol. 7, Ref. E-II-7*, 443-447.

Harold, J. H., & FICS, F. (1997). Data Encryption: A Non-Mathematical Approach. *Computers & Security*, 370.

Markagić, M. S., & Markagić, M. M. (2013). Osnove savremene kriptoanalize. *Konferencija o bezbednosti informacija BISEC 2013*, 59.

Mašović, S., Saračević, M., & Zornić, D. (2011). Bezbednost podataka u vpn-u na javnoj globalnoj mreži. *Međunarodna konferencija E-trgovina*, 1, 4.

Pleskonjić, D., Maček, N., Đorđević, B., & Carić, M. (2007). *Sigurnost računarskih sistema i mreža.* Beograd: Mikro knjiga.

Poljak, D. (2006). *Strategija obrane od linearne i diferencijalne kriptoanalize.* Zagreb: Sveučilište u Zagrebu.

Datum prve prijave: 23.05.2015.
Datum prijema korigovanog članka: 22.09.2015.
Datum prihvatanja članka: 22.10.2015.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*
Cvetković, T., Mihajlović, M., & Miladinović, Ž. (2016, januar 15). Izbor metode kriptovanja podataka u bežičnim računarskim mrežama. (Z. Čekerevac, Ur.) *FBIM Transactions, 41*, 19-27. doi:10.12709/fbim.04.04.01.03

*Style – **Chicago** Sixteenth Edition:*
Cvetković, Tamara, Milan Mihajlović, i Živanka Miladinović. 2016. „Izbor metode kriptovanja podataka u bežičnim računarskim mrežama.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 41: 19-27. doi:10.12709/fbim.04.04.01.03.

*Style – **GOST** Name Sort:*
Cvetković Tamara, Mihajlović Milan i Miladinović Živanka Izbor metode kriptovanja podataka u bežičnim računarskim mrežama [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 januar 2016. - T. 41. - str. 19-27.

*Style – **Harvard** Anglia:*
Cvetković, T., Mihajlović, M. & Miladinović, Ž., 2016. Izbor metode kriptovanja podataka u bežičnim računarskim mrežama. *FBIM Transactions,* 15 januar, Tom 41, pp. 19-27.

Style – **ISO 690** Numerical Reference:
Izbor metode kriptovanja podataka u bežičnim računarskim mrežama. **Cvetković, Tamara, Mihajlović, Milan i Miladinović, Živanka.** [ur.] Zoran Čekerevac. Beograd : MESTE, 15 januar 2016, FBIM Transactions, T. 41, str. 19-27.