KRIPTOGRAFIJA U FUNKCIJI SIGURNOSTI INFORMACIONIH SISTEMA

CRYPTOGRAPHY IN THE FUNCTION OF INFORMATION SYSTEMS SECURITY

Džemal Kulašin
Ekonomska škola Travnik
Travnik

Hadžib Salkić
Sveučilište/Univerzitet “Vitez”
Vitez

REZIME
U posljednje vrijeme, svjedočimo sve učestalijim manifestacijama cyber kriminala, koji svojim pojavnim oblicima i razmjerama ozbiljno ugrožava poslovne sisteme uzrokujući respektabilne finansijske troškove. No, i pored nepobitnih statističkih pokazatelja o finansijskim gubicima, čini se da nije u dovoljnoj mjeri sazrijela svijest o informacijskom integritetu, niti se sigurnosnim aspektima informacionih sistema posvećuje dovoljna pažnja.
Cilj ovog rada je ukazivanje na kriptografiju kao specifičnu naučnu disciplinu, odnosno razmatranje određenih kriptografskih formi uz njihovo anagažiranje u funkciji sigurnosti informacionih sistema.

Ključne riječi: kriptografija, digitalni potpis, PGP

SUMMARY
Lately, we are witnesses of more and more frequent manifestations of cyber crime, which in its forms and dimensions seriously endangers business systems and causes significant financial costs. However, despite the undeniable statistical indicators on financial losses, it seems that the consciousness on information integrity is not yet sufficiently developed, nor is sufficient attention given to the security aspects of information systems.
The objective of this paper is to point to cryptography as a specific scientific discipline, namely the consideration of specific cryptographic forms with their engagement in the function of information systems security.

Keywords: cryptography, digital signature, PGP

1. UVOD

Pojmovno određenje računarskog kriminaliteta još uvijek nije usuglašeno, tako da se mogu čuti različiti termini: računarska zloupotreba (computer abuse), kriminal povezan sa računarom (computer related crime), računarske prevare (computer fraud) te najčešći termin računarski kriminal (computer crime). Bez obzira na pojmovno određenje, ova vrsta kriminala označava protupravne povrede imovine, kod kojih se računarski podaci s predumišljajem mijenjaju, razaraju, do njih neovlašteno dolazi i koristi ili se koriste zajedno sa hardverom [5].

U ovim terminološkim dilemama, očito, nedostaje termin cyber kriminal, koji možemo objasniti kao računarski kriminal prisutan u cyber prostoru, kojemu su osnova djelovanja računarske mreže, a posebno Internet. A upravo terminološki "zaboravljeni" cyber kriminal postaje globalna prijetnja ekonomskim tokovima, što potvrđuju činjenice da godišnji troškovi uzrokovani ovom vrstom kriminalnih radnji iznose oko 114 milijardi američkih dolara. No, to je tek dio mozaika, jer predstavlja samo direktno izazvanu štetu uz trošak "borbe" protiv počinitelja; ukupna šteta zbog izgubljenog vremena usljed cyber napada kompanije procjenjuju na čak 274 milijarde dolara, što znači da ukupna procjena šteta na godišnjem nivou iznosi cijelih 388 milijardi dolara [7].

Ovakvi podaci, donekle, i nisu začuđujući, jer su savremene organizacije potpuno ovisne o informacionim sistemima koji se nužno moraju vezati za Internet, te su i najranjivije upravo na različite napade iz cyber prostora [3]. Dodamo li ovome i činjenicu da se u praksi korisnici informacionih sistema (tj. uposlenici) s pravom oslanjaju na (ponekad nedostatnu) tzv. industrijsku sigurnost [2], dolazimo do spoznaje zašto se vrata na koja kucaju cyber kriminalci relativno lako otvaraju.

Stoga je jasno da se u strategiji sigurnosti informacionih sistema, pored antivirusnih alata i firewall-a kao prvih linija odbrane informacionih sistema, trebaju uključivati i dodatne tehnike, posebno u cilju očuvanja tajnosti povjerljivih podataka. Jedna od mogućih solucija je kriptografija, odnosno implementacija pojedinih kriptografskih sistema kojima se može utjecati na glavne aspekte informacijske sigurnosti prema standardu ISO 27001, a to su: (a) **očuvanje tajnosti informacije** (do informacije i njene upotrebe mogu doći samo ovlašteni korisnici), (b) **očuvanje cjelovitosti informacije** (informacija u formi i sadržaju se ne smije promijeniti bez znanja vlasnika informacije, što uključuje i metode i postupke obrade informacija) i (c) **osiguranje dostupnosti informacije** (do informacije moraju moći doći svi ovlašteni korisnici tamo gdje i kada im treba u prihvatljivom obliku) [8].

2. POJAM I ZNAČAJ KRIPTOGRAFIJE

Kriptografija je naučna disciplina koja se koristi složenim matematičkim principima u generiranju ključeva kojima se u maksimalno mogućoj mjeri osigurava informacijska sigurnost. Prvi kriptografski pokušaju zabilježeni su još prije 4000 godina, gdje su "ključevi" za kodiranje poruka bili jednostavna zamjena pozicije slova, po čemu je čuvena Cezareva kriptografija. U savremenom kodiranju poruka, tj. za prevođenje poruka iz otvorenog (nešifriranog) oblika u šifrirani oblik, kriptografija se danas oslanja na kriptografske algoritme. Dva dominantna kriptografska algoritma su: (1) simetrični algoritam, pogodan za zaštitu datoteka i foldera, gdje se isti ključ koristi za šifriranje i dešifriranje teksta te (2) asimetrični algoritam, pogodniji za zaštitu u elektronskoj komunikaciji, gdje se tzv. javni ključ (Public key) koristi za šifriranje, dok se tzv. privatni ključ (Private key) koristi za dešifriranje.

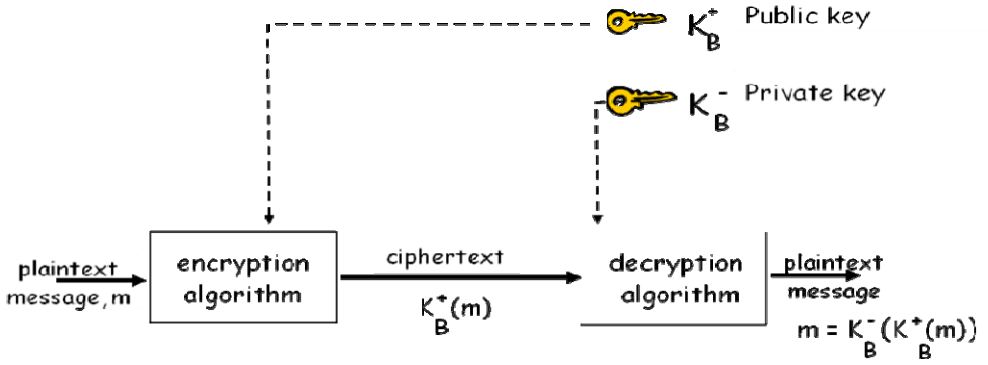
Ovdje je, naravno, riječ o kriptografiji usko vezanoj sa uznapredovalom računarskom tehnologijom, jer su razvojem računarske tehnologije drastično porasle i kriptografske mogućnosti, posebno u pogledu generiranja višebitnih, jakih ključeva. Općenito, snaga ključa procjenjuje se po tome koliko treba komercijalno dostupnom računaru da dešifrira šifriranu poruku tzv. napadom golom silom (brute force). Danas se 40-bitni ključevi smatraju beskorisnim, 128-bitni, 256-bitni i 512-bitni ključevi su industrijski prihvatljivi, dok 1024-bitni i 2048-bitni ključevi nude maksimalnu sigurnost [1]!?
Gdje u svakodnevnoj praksi uviđamo potrebu za kriptografijom? Navest ćemo dva slučaja.

1) Povjerljivi podaci, kao što su JMBG djelatnika, brojevi kreditnih kartica i sl. pohranjuju se na nosioce memorije, ali nekad zaštićeni slabim lozinkama koje se mogu dešifrirati čak i potpuno besplatnim programima za razbijanje šifri dostupnim na pojedinim web lokacijama na Internetu.
2) Slanje povjerljivih podataka postojećim komunikacijskim kanalima informacionih sistema, a posebno servisima Interneta (npr. E-mail) često se vrši u duhu rutinske neobavezne konverzacije, nezaštićeno.

Kriptografsko rješenje ovdje je tzv. kriptografija u javnom domenu, koja obuhvata standarde i protokole nastale kao rezultat pojedinačih ili korporativnih aktivnosti koji su dati na korištenje najširoj javnosti. Najpoznatija javna kriptografska inicijativa svakako je PGP (Pretty Good Privacy) kao de-facto standard u oblasti kriptozaštite, koji je vezan sa metodologijom digitalnog potpisa.

2.1. Digitalni potpis

Digitalni potpis predstavlja kriptografski sistem analogan svojeručnom potpisu tekstualnih (printanih) dokumenata. U osnovi digitalnog potpisa je asimetrični algoritam, pri čemu se otvorena, početna poruka (plaintext) od strane pošiljaoca šifrira javnim ključem (Public key) onome kome se poruka šalje, postajući šifrirana poruka (ciphertext). Takvu šifriranu poruku može dešifrirati samo vlasnik privatnog ključa (Private key), koji sadrži dekripcijski algoritam koji poruku ponovo transformira u tzv. plaintext, tj. početnu poruku (Slika 1).



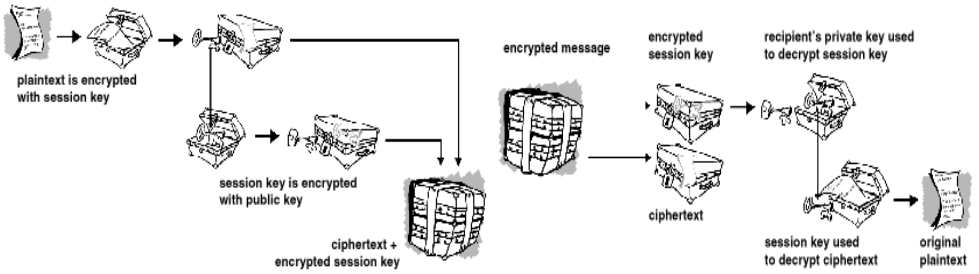
Slika 1. Šema asimetričnog algoritma [6]

U ovakvoj zaštiti i autentikaciji komunikacije, problem je povjerenje javnog ključa, odnosno kako vjerovati da je javni ključ siguran i da pripada osobi ili instituciji sa kojom se uspostavlja zaštićena komunikacija? Problem je riješen uspostavljanjem organizacija od povjerenja tzv. CA organizacija (Certification Authority), koje garantuju da je javni ključ u potpunosti siguran, i da bez dvojbi pripada osobi ili instituciji iza koje CA organizacija stoji. Zadatak ovih organizacija je da osobama/institucijama koje dostave svoje podatke kreiraju digitalne certifikate, te ih vežu javnim ključem. Vrijedi napomenuti da među CA organizacijama u svijetu, najveće povjerenje uživa VeriSign [1].

2.2. PGP (Pretty Good Privacy)

Shodno važećim zakonima, američka vlada je svojevremeno podigla tužbu protiv Philla Zimmermanna kada je 1991. godine publicirao PGP kao kriptografski program sa (do tada) neviđenim nivoima enkripcije podataka u javnom prostoru. Ipak, tužba je kasnije povučena, a PGP je za kratko vijeme stekao ogroman broj poklonika koji su bili spremni ne samo da ga koriste, već i dalje razvijaju. Tako je PGP program za kratko vrijeme napravio značajne

pomake od izvornog Zimmermannovog koda, postavši dostupan i u besplatnoj (freeware) verziji sa grafičkim sučeljem.
Kako radi PGP? Na strani pošiljatelja, u prvom koraku enkripcije PGP komprimira tekst smanjujući veličinu podataka koji se prenose. U drugom koraku, stvara se tzv. session key tako da se analiziraju slučajni uzorci kao što je npr. pomjeranje miša ili broj pritisnutih tipki. Njime se enkriptira plaintext, dok se session key kriptira javnim ključem što se zajedno mrežom šalje do primatelja. Na strani primatelja, vrši se otključavanje poslanog paketa, tako što se prvo otključava mala "bravica" odnosno čita se session key, koji sadrži ključ za dekriptiranje cijelog teksta (Slika 2) [9].

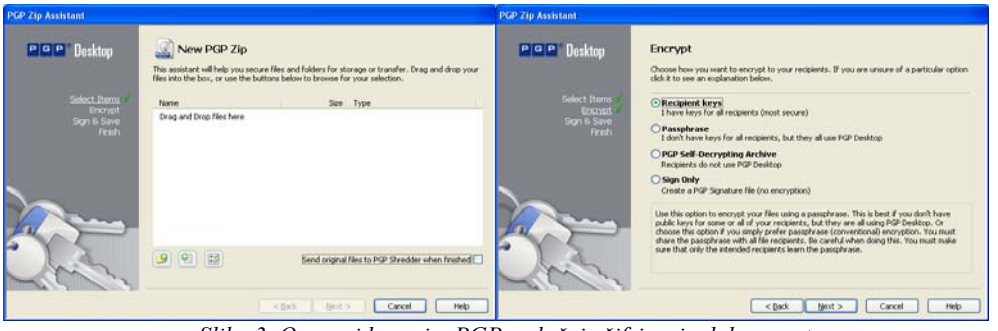


Slika 2. Koraci PGP-a na strani pošiljatelja (lijevo) i primatelja (desno) [9]

Kako se može uočiti, PGP u funkcionalnom smislu kombinira najbolje osobine simetričnog i asimetričnog algoritma, kao dva glavna kriptografska algoritma. Zbog toga je PGP u formi dodatka E-mail klijentima izrastao u de-facto standard u oblasti sigurnosti elektronske komunikacije [4], što se itekako može i treba koristiti u svakodnevnoj poslovnoj praksi.

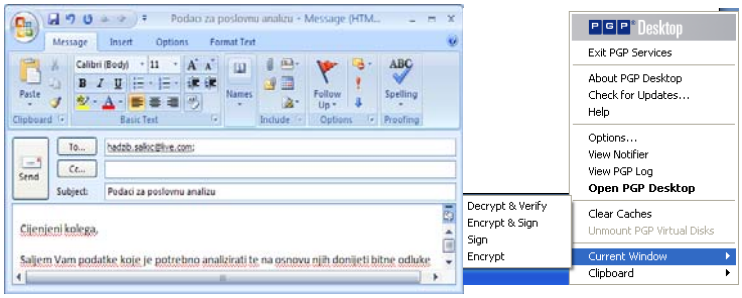
2.3. Primjeri primjene PGP-a u svakodnevnoj praksi

Primjer 1. U slučaju pohranjivanja povjerljivih podataka na nosiocima memorije, potrebno je da provedemo sljedeće korake: a) pozovemo opciju New PGP Zip, b) odaberemo folder sa datotekama koje želimo šifrirati te c) odaberemo način enkripcije (Slika 3). Najsigurniji način zaštite je prva ponuđena opcija Recipient keys, pogodnija za kasniji mrežni transfer podataka (file attachment), koja podrazumijeva da smo u PGP-u ranije generirali ključeve (keyring). Druga ponuđena opcija je Passphrase, koja pruža dovoljan nivo zaštite povjerljivih podataka u slučaju njihovog internog čuvanja na disku računara.



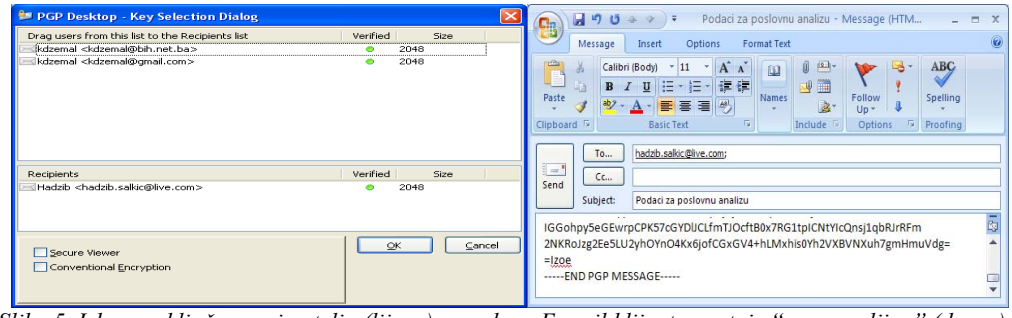
Slika 3. Osnovni koraci u PGP u slučaju šifriranja dokumenata (izvor: screenshots)

Primjer 2. U slučaju slanja povjerljivih poruka servisima Interneta, odnosno šifriranja elektronske komunikacije potrebno je da provedemo sljedeće korake: a) kreiramo poruku E-mail klijentom (npr. MS Outlook), b) uz **aktivan** prozor aplikacije E-mail klijenta pozovemo PGPtray, gdje odaberemo opcije Current Window - Encrypt & Sign (Slika 4).



Slika 4. Aktivan prozor E-mail klijenta (lijevo) i opcije PGPtray-a (desno) (izvor: screenshots)

Potom je potrebno odabrati javni ključ primatelja (principom Drag and Drop) kojim PGP vrši šifriranje poruke, nakon čega otvorena poruka sa povjerljivim sadržajem postaje "nerazumljiva", tj. šifrirana (Slika 5).



Slika 5. Izborom ključeva primatelja (lijevo), poruka u E-mail klijentu postaje "nerazumljiva" (desno) (izvor: screenshots)

Na strani primatelja proces se svodi na izbor opcije Decrypt iz PGPtray-a, čime "nerazumljiva" poruka sa povjerljivim podacima postaje "razumljiva", tj. dešifrirana. Naravno, za ovakvu šifriranu PGP komunikaciju potrebno je da obe strane (pošiljalac i primatelj) imaju instaliran PGP[1] te da su prethodno generirali i razmijenili (javne) ključeve.

3. ZAKLJUČAK

Što je organizacija ovisnija o informacionim sistemima, to je i ranjivija na različite napade koji ugrožavaju sigurnost informacionih sistema, a time i tajnost povjerljivih podataka. Povećanje rizika posebno dolazi do izražaja zbog nužnosti spajanja lokalnih mreža sa javnim mrežama, kao što je Internet, kada govorimo o cyber kriminalu. Ipak, i pored dramatičnih statističkih pokazatelja o razmjerama cyber kriminala, (čini se) još uvijek nije u dovoljnoj mjeri sazrijela svijest o (o)čuvanju informacijske sigurnosti, a korisnici informacionih sistema u svakodnevnoj praksi isuviše se oslanjaju na tzv. industrijsku sigurnost. Tim više su

[1] Freeware verzija PGP ne omogućava šifriranje E-mail poruka, i potrebno je kupiti licencu.

organizacije usmjerenije ka sistemu upravljanja informacijskom sigurnošću (ISMS) kojim se osigurava ispunjenje zahtjeva na očuvanju glavnih aspekata informacijske sigurnosti tzv. C-I-A (**C**onfidentiality - tajnost, **I**ntegrity - cjelovitost i **A**vailability - dostupnost), regulirano serijom standarda ISO 27000.

U ovom radu naveli smo samo dva praktična slučaja gdje uviđamo potrebu za kriptografijom: prvi slučaj je spremanje povjerljivih podataka na medije zaštićeno slabim lozinkama, dok je drugi slučaj transfer povjerljivih podataka cyber prostorom u nešifriranom obliku. Kvalitetno kriptografsko rješenje u ovim radnjama je PGP kao de-facto standard u oblasti kriptozaštite uz digitalni potpis kao uvjet šifriranog komuniciranja, ali i uvjet autentikacije učesnika u elektronskoj komunikaciji. Primjenjujući ove kriptografske forme, povjerljivi podaci u vlasništvu pojedinca ili organizacije, bilo da je riječ o njihovom spremanju na medije ili transferu u cyber prostoru, bit će zaštićeni jakim ključevima koje u razumnom vremenu i razumnom računarskom tehnikom nije moguće dešifrirati.

Na kraju, potrebno je ukazati i na oprez u kriptografskom smislu, jer pored nepobitne koristi primjene kriptografije u zaštiti povjerljivih podataka, postoji (na žalost) i jedna druga strana, u kojoj se kriptografski softver nastoji iskoristiti suprotno svrsi o kojoj je riječ u ovom radu.

4. LITERATURA

[1] Murray, A.C, Weafer, V. (2006): Sigurni na Internetu, MIŠ, Zagreb.
[2] Rainer, R, K., E, Turban (2009): Uvod u informacione sisteme – Podrška i informatizacija poslovanja, Datastatus, Beograd.
[3] Lagumdžija, Z. (2005): Menadžment informacioni sistemi, Ekonomski fakultet, Sarajevo.
[4] Babić, V. (2009). Kompjuterski kriminal, RABIC, Sarajevo.
[5] Hanić, H., Sućeska, M. (2008): Kompjuterski kriminal - pojavni oblici i preventiva, Fakultet kriminalističih nauka, Sarajevo.
[6] Pastore, M., Dulaney, E. (2007): Security+, Kompjuterska biblioteka - Sybex, Beograd.
[7] Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu (2012): Profiliranje cyber kriminalaca, [Internet], Dostupno na: http://www.cis.hr/files/dokumenti/CIS-DOC-2012-01-038.pdf [Pristupljeno 11.04.2013].
[8] Saša Aksentijević, Kvalis – Portal za kvalitetu i sigurnost (2009): ISMS - Informacijska sigurnost [Internet], Dostupno na: http://www.kvalis.com/component/k2/itemlist/category/36-isms-informacijska-sigurnost [Pristupljeno 30.04.2013].
[9] Krešimir Dujmić, Fakultet Elektrotehnike i računarstva Sveučilišta u Zagrebu (2012). Kriptografija (PGP), [Internet], Dostupno na: http://fly.srk.fer.hr/~peloquin/PGP [Pristupljeno 13.04.2013].