1. Primjena inteligentnih kartica u zaštiti računarskih mreža

Predmet ovog rada je tehnologija inteligentnih kartica i način na koji se one primjenjuju u zaštiti računarskih mreža.

Inteligentna kartica, veličine i oblika kreditne kartice, obično sa ugrađenim integralnim kolom, predstavlja vrlo pogodan alat za obezbjeđenje sigurnosti, čuvanje podataka i druge posebne namjene. Da bi se mogli odbraniti od neprijatelja, potrebno ga je prvo definisati. Stoga se postavlja pitanje, šta utiče na bezbjednost informacija, koji su to oblici ugrožavanja podataka koji nose informaciju, a samim tim i računarskih mreža kao medija za njihov prenos.

Izložene su osobine inteligentnih kartica i predstavljena njihova uloga u sistemima za zaštitu računarskih mreža i PC sistema. Inteligentna kartica obezbjeđuje različite opcije nivoa sigurnosti, koje se kreću od jednostavne kontrole pristupa, pa sve do zaštite složenih sistema primjenom različitih algoritama za šifrovanje i posebnim načinom komunikacije između korisnika jednog takvog sistema.

Inteligentne kartice su se pokazale kao pogodan medij za obavljanje različitih transakcija, autorizaciju i identifikaciju. Pošto se sposobnosti i mogućnosti ovih kartica povećavaju iz dana u dan, došli smo u situaciju da se jedna inteligentna kartica višestruko primjenjuje, tj. da može zamjeniti kompletan sadržaj našeg novčanika, uključujući kreditne kartice, vozačku dozvolu, gotovinu, propusnice za pristup objektima ili računarskoj mreži, pa čak i kompletan zdravstveni karton korisnika. Sadržavajući različite sertifikate, ove kartice možemo koristiti za identifikaciju, bez obzira gdje se nalazimo i šta želimo da radimo.

2. BEZBJEDNOST INFORMACIJA (*Information Security*):

2.1. Prijetnje i mehanizmi zaštite

Mada je bezbjednost informacija uvijek imala važnu ulogu, tek u zadnjih 5 godina se pojavila prava eksplozija zahtjeva za bezbjednošću servisa. Smatra se da je razlog tome brzi razvoj *internetworking* sistema, a posebno Interneta. U slijedećem dijelu navešćemo neke od najčešćih prijetnji i opasnosti, koje se skrivaju u komunikacionim sistemima, kao i tehnologije za bezbjednost informacija koje su usmjerene za borbu protiv tih opasnosti.

2.1.1. Prijetnje (Threats)

Osnovne kategorije prijetnji su:

- hakerisanje i upadi (*Hacking and Intrusion Attacks*): ova kategorija obuhvata napade, kada uljez u sistemu dobija pristup nekom području ili resursima. Klasični primjer je oštećivanje web stranice ili krađa povjerljivih podataka neovlaštenim upadom.
- virusi i crvi (*Viruses and Worms*): oni rade na principu maskiranja (prerušavanja) zlonamjernog koda ili programa i obmane naivnog, nesumnjičavog korisnika, koji izvrši taj kod. Jednom kada se pokrene program, virusi preuzimaju mašinu, šire, uništavaju ili mijenjaju informaciju.
- osporavanje servisa (*Denial-of-Service*): u ovu kategoriju spadaju svi napadi usmjereni na ometanje servisa. Oni često koriste poznate slabosti kako bi srušili sistem ili podsistem. Npr. fijuk smrti (*Ping of Death*) iskorištava uobičajene previde, propuste u steku internet protokola (IP). Tada jako veliki, ogroman paket obara mrežni podsistem. Drugi pristup, koji se često koristi je bombardovanje sistema (tipično servera) do te mjere da on ne može više normalno posluživati zahtjeve korisnika.
- prisluškivanje (*Eavesdropping*): napadač sluša ili posmatra tok informacija. U ovu svrhu se koriste različiti uređaji za prisluškivanje (*Wiretaps*).
- aktivni napadi (*Active Attacks*): kao kod prisluškivanja, vrši se presretanje informacija u tranzitu. Za razliku od pasivnog nadgledanja ili sakupljanja informacija, podaci se presreću, mijenjaju i ponovo šalju (komunikaciona linija je prekinuta i usmjerava se preko napadača).

- lažno predstavljanje (*Spoofing Attacks*): kod takvih napada, osoba ili mašina se lažno predstavlja da bi dobila pristup resursima.
- ponavljanje napada (*Replay Attacks*): napadi se često baziraju na ponovljenom slanju paketa koji su već primljeni na prijemnoj strani. Npr. ako se šalje poruka u banku sa instrukcijom da se doda 1000 KM na bankovni račun, tada je svakako u interesu imaoca računa da taj postupak, tj. poruku ponovi još nekoliko puta.
- zamjena paketa (*Packet Alteration*): umjesto lažnog identiteta, napadač može da iskoristi validnu konekciju i da istu prilagodi svojim potrebama. Npr. ako se pošalje email koji kaže ″gospodinu X više nije dozvoljen pristup u objekat Y″, onda zamijeni ″objekat Y″ sa ″objekat Z″, može se desiti da se gospodinu X dozvoli pristup objektu Y.
- i posljednja kategorija, mada se ne odnosi na kriptografiju, je ona koja koristi najslabije tačke većine bezbjedosnih sistema, a to su korisnici i administratori sistema.

Postoji nebrojivo mnogo varijacija i kombinacija tipova napada, koji prijete informacijama i informacionim sistemima. Na sreću, industrija posjeduje mnogo različitih alata za borbu protiv takvih prijetnji.

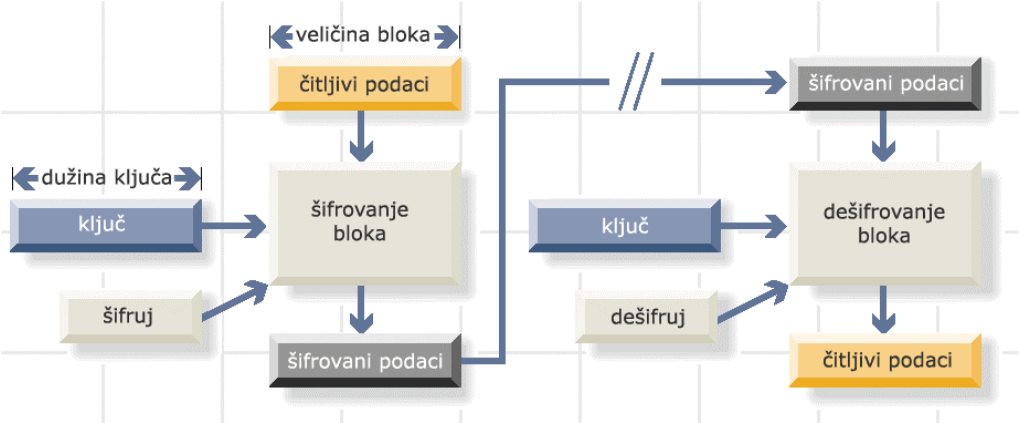
2.2. Mjere bezbjednosti

Postoje brojna područja istraživanja i tehnologije koje se odnose na bezbjednost informacionih resursa.Veliku trojku čine: tajnost (*Confidentiality*), integritet (*Integrity*) i autentičnost (*Authentication*).

2.3. Kriptologija

Šifrovanje

Moderni sistemi koriste snažne algoritme za šifrovanje, skremblovanje i deskremblovanje informacija. Ovi sistemi spadaju u neku od slijedećih kategorija. Slijedeća slika prikazuje sistem za šifrovanje koji koristi simetrično blok šifrovanje:



Slika 1 - principi šifrovanja i dešifrovanja

Algoritmi koji se koriste su veoma različiti, različitih nivoa sigurnosti, brzine, veličine bloka i dužine ključa. Npr. DES je prilično skroman po pitanju sigurnosti po današnjim standardima, relativno se sporo softverski pokreće, ali je hardverski vrlo efikasan i on ima veličinu bloka 64 bita i dužinu ključa 56 bita. Sistemi šifrovanja i dešifrovanja će biti kasnije objašnjeni u ovom radu. Slijedeća tabela pokazuje glavne simetrične i asimetrične algoritme za šifrovanje:

	simetrični algoritmi	asimetrični algoritmi
blok	DES, 3DES, RC2, RC5, AES, CAST, IDEA, Skipjack, Safer, Blowfish, FEAL	RSA
stream (sekvencijalni)	RC4, A5 (GSM), Rambutan	BBS

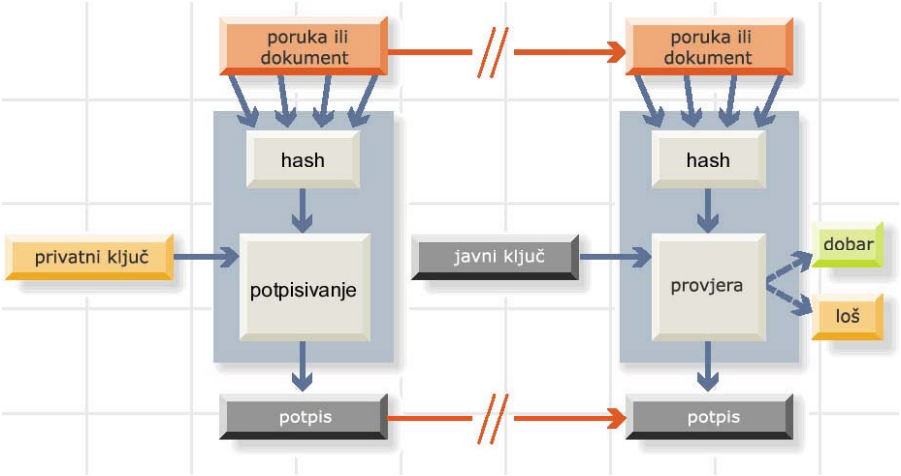
Tabela 1 - algoritmi za šifrovanje

Hash algoritam (message digest)

Iako se digest (*hash*) uveliko primjenjuje, većina primjena se odnosi na otkrivanje da li je informacija netaknuta. Kriptografski digest uzima različitu veličinu bloka podataka na ulazu i proizvodi poruku specifične veličine, zavisno od upotrijebljenog algoritma. Priroda algoritama je takva da ne postoje dva ulazna bloka koji mogu dati isti rezultat. Ova zaštita je usmjerena protiv napadača koji žele da promijene ili zamijene datoteke koje primalac treba da provjeri na osnovu već poznate hash vrijednosti. Najpopularniji sistemi ovog tipa su MD4, MD5 i SHA-1.

Digitalni potpis

Sistemi za digitalno potpisivanje generalno koriste asimetrične ključeve da izvrše svoje operacije, a to su: funkcija potpisivanja upotrebom privatnog ključa i verifikacija korištenjem javnog ključa. Slijedeća slika prikazuje pošiljaoca, na lijevoj strani, koji šalje vjerodostojnu datoteku do primaoca na desnoj strani. Da bi postigli ovo, pošiljalac potpisuje hash vrijednost korištenjem privatnog ključa koji je poznat samo pošiljaocu i šalje potpis sa datotekom. Kada primalac dobije ovakvu poruku izvršava se verifikacija koja određuje da li je potpis važeći ili ne.



Slika 2 - Upotreba digitalnog potpisa

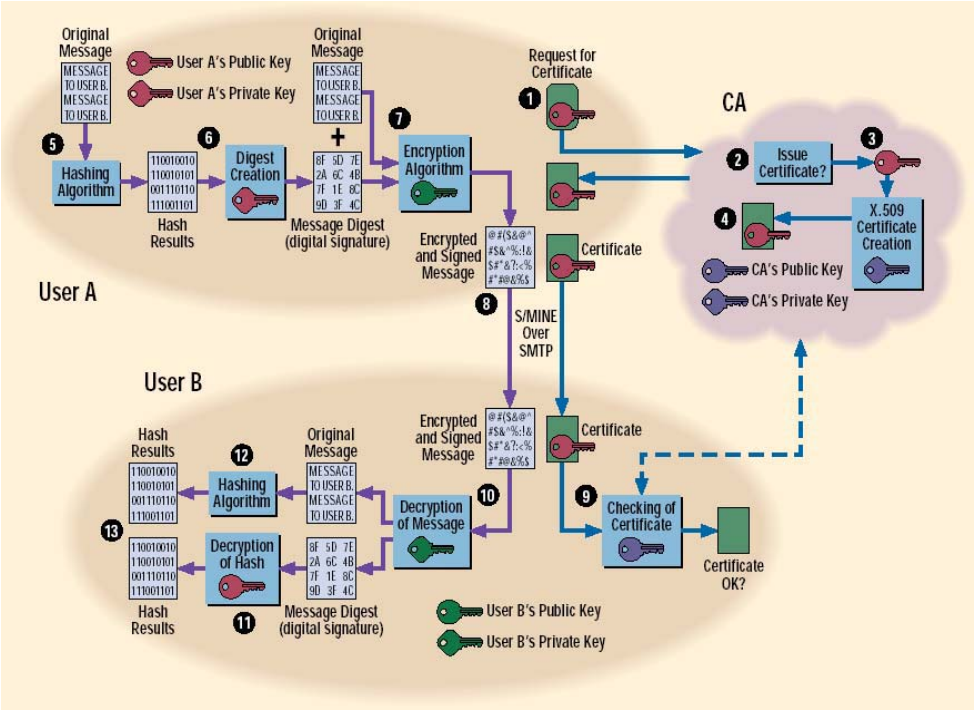
Treba uočiti interesantnu primjenu digitalnog potpisa pomoću koje se distribuira softver bez virusa. Ako se neki izvršni program potpiše od strane kompanije kojoj vjerujemo, onda možemo verifikovati potpis da se uvjerimo da on nije bio inficiran od svog nastanka. RSA i DSA su dva najčešće korištena sistema za digitalno potpisivanje. Digitalni potpisi se koriste da omoguće autentičnost (vjerodostojnost). Problem je kako primaoc poruke dobije javni ključ.

Diffie-Hellman ključ

Ovo je popularni metod koji predstavlja jedan hibridni sistem u kojem se ključevi razmjenjuju korištenjem asimetričnih sistema za šifrovanje. Ove ključeve naizmjenično koriste brzi simetrični sistemi.

PKI (Public Key Certificate)

Sertifikat je digitalni identitet autorizovan od povjerljive asocijacije, poznatog kao Certificate Authority (tijelo za izdavanje sertifikata). Generalno, on služi za digitalno povezivanje vlasnika sa javnim ključem. Nakon što se sertifikat potpiše, on ne može biti promijenjen. Struktura sertifikata se organizuje u skladu sa standardom ITU X.509. Sertifikati uključuju identifikatora, javni ključ, serijski broj, datum do kada važi i potpis generisan upotrebom privatnog (tajnog) ključa ovog tijela. Primjer sertifikata javnog ključa je dat na slijedećoj slici:



Slika 3 - Primjer primjene sertifikata

Popularnost sertifikata javnih ključeva uveliko raste pošto se koriste za elektronsku trgovinu, siguran e-mail, elektronske formulare, virtuelne privatne mreže itd. Sada kada imamo tehnologiju koja može odrediti ko je ko, slijedeći korak je da vidimo šta je kome dozvoljeno da uradi. Ovo je glavna razlika između autentičnosti i autorizacije. Kada neko pokuša da pristupi datoteci na serveru potrebno je odlučiti da li taj neko posjeduje pravo pristupa. To nije tako jednostavno. Serveri mogu imati liste sa istorijom kontrole pristupa, ali većina organizacija koristi *firewall*.

Mada se funkcije sigurnosti u *firewall*-u manje odnose na kriptografiju, one su ekstremno bitne u jačanju sigurnosne politike. *Firewall* se razvija između mrežnih domena za izolaciju jednog od drugih, dozvoljavajući diskretan pristup u skladu sa nekom procedurom. Oni često analiziraju mrežni saobraćaj na osnovu poznatih protokola da se osiguraju da se saobraćaj odvija kao što bi trebao. Tako npr. *firewall* može dozvoliti saobraćaj od jednog do drugog domena, ali samo ako je sesija inicirana od određene strane. *Firewall* takođe može provjeriti podatke u aplikacijama kako bi filtrirao sadržaj ili da otkrije viruse.

Kontramjere

Kontramjere mogu biti svrstane u dvije grupe: one koje sprečavaju (*preventive*) ili koje otkrivaju (*detective*). Sada ćemo nabrojati neke od njih:

- autentičnost,
- digitalni potpis,
- kontrola pristupa,
- virtuelne privatne mreže (VPN),
- šifrovanje,
- otkrivanje upada (uljeza),
- provjera i prijavljivanje (*logging*),
- nemogućnost odbijanja (*non-repudiation*).

Preporučuje se da operativni sistemi korišteni u elementima NGN mreža imaju sigurnost konfigurisanu kao osnovnu kontramjeru:

- sve neesencijalne pogodnosti (npr. TCP/UDP portovi) trebaju biti onemogućene,
- daljinski pristup takođe treba biti onemogućen. Ako je ovo neophodno, sve aktivnosti trebaju biti provjerene.
- server koji kontroliše operativni sistem mora biti zaštićen,
- kompletan sistem zasnovan na prijavljivanju i provjeri. Učestalo nadgledanje datoteke za prijavljivanje je preporučljivo.

Takođe se preporučuje da sama mreža posjeduje sigurnu konfiguraciju. Operator bi trebao da:

- promijeni podrazumijevajuće lozinke,
- onemogući neiskorištene portove,
- održava listu lozinki za prijavljivanje,
- koristi autentifikaciju entiteta,
- kontroliše sigurnost konfiguracije.

2.4. Kriptologija

Kriptologija je termin koji potiče od grčkih riječi kriptos (tajan, skriven) i logos (nauka) i označava naučnu disciplinu koja se bavi bezbjednim (tajnim) komunikacijama.

Problemi integriteta informacije rješavaju se u okviru kriptografije, tj. kriptotransformacija informacije.

U okviru klasične kriptografije (kriptografija na osnovu tajnog ključa) postoji samo jedan dio privatne ili tajne informacije - ključ - pomoću koga izvor pretvara informaciju u šifru, a odredište, šifru u informaciju. To je tzv. proces šifrovanja i dešifrovanja. Tako dobijamo šifrovani tekst - **šifrat**. Kada se ne poznaje šifra tada se šifrat zove **kriptogram**. Zato se, pored pojma dešifrovanja uvodi pojam dekriptovanje, kao postupak da se do otvorenog teksta poruke dođe i bez poznavanja šifre, odnosno transformacije kojom je otvoreni tekst preveden u šifrat.

U kriptografiji sa javnim ključem postoje dva dijela informacije, pri čemu je bar jedan dio nemoguće računskim putem otkriti na osnovu poznavanja drugog dijela. Jedan dio je dodatna informacija (ključ), koju koristi izvor da bi šifrovao informaciju čiji integritet štiti, a drugi dio je dodatna informacija (ključ), koju koristi odredište radi operacija nad rezultirajućom šifrom. Zavisno od aplikacija, oba dijela ove informacije ne moraju se čuvati u tajnosti.

Ako je računskim putem nemoguće otkriti ključ za dešifrovanje na osnovu ključa za šifrovanje, tada se ključ za šifrovanje ne mora držati u tajnosti. Međutim, on se mora zaštititi od supstitucije ili modifikacije, jer bi se moglo desiti da izvor koristi lažan ključ za koji protivnik (nepoželjnik) posjeduje odgovarajući ključ za dešifrovanje. Ključ za dešifrovanje mora se držati u tajnosti i fizički obezbijediti od supstitucije ili modifikacije.

Kod kriptografije sa jednim ključem, predajnik i prijemnik nemaju drugog izbora, već da ograničeno vjeruju jedan drugom. Kod kriptografije sa dva ključa, samo jedan od učesnika (predajnik ili prijemnik) je sa neograničenim povjerenjem. Međutim, postoje aplikacije u kojima se ni jednom od učesnika ne može neograničeno vjerovati. Tada su obično neki nepoznati elementi u sistemu sa neograničenim povjerenjem (arbitri u sistemu).

Razvoj algoritama za javno korištenje se odvija potpuno javno. Razvijeni su i mnogi kvalitetni kriptoalgoritmi na bazi dva ključa, ali i niz metoda za razbijanje šifri, tj. za kriptoanalizu.

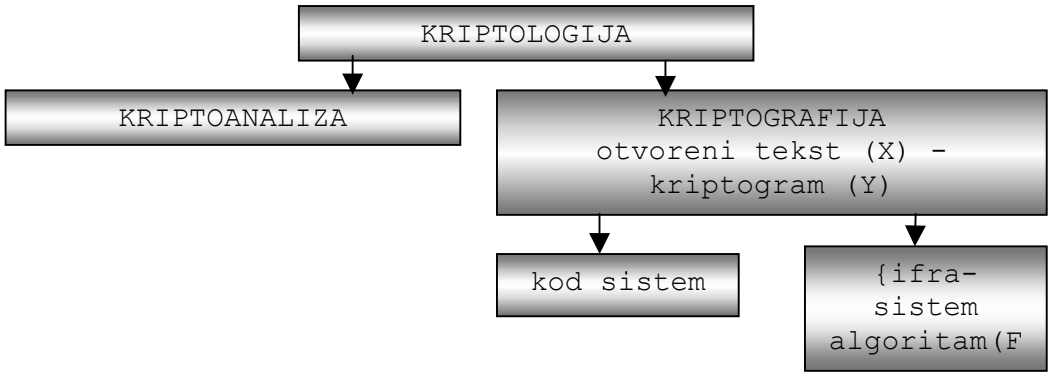
Definisanje dobrih kriptotransformacija, tj. algoritama nije jedini kriptografski problem. Ostaje problem distribucije ključeva koji je inicirao razvoj kriptografije sa jednim ključem. Organizacijom distribucije ključeva definišu se načini preuzimanja privatnog dijela informacije (ključa) i garantovanja njenog integriteta.

Na nivou informacionog sistema (u širem smislu) sa kriptozaštitom, mogući su i problemi sa greškom u protokolu. Greške u protokolu su rezultat kriptoanalize na nivou sistema umjesto na nivou algoritma. Zbog toga je poželjno da se povjerljiva informacija prenosi različitim kanalima u sistemu.

2.4.1. Kriptografija kao mjera sigurnosti

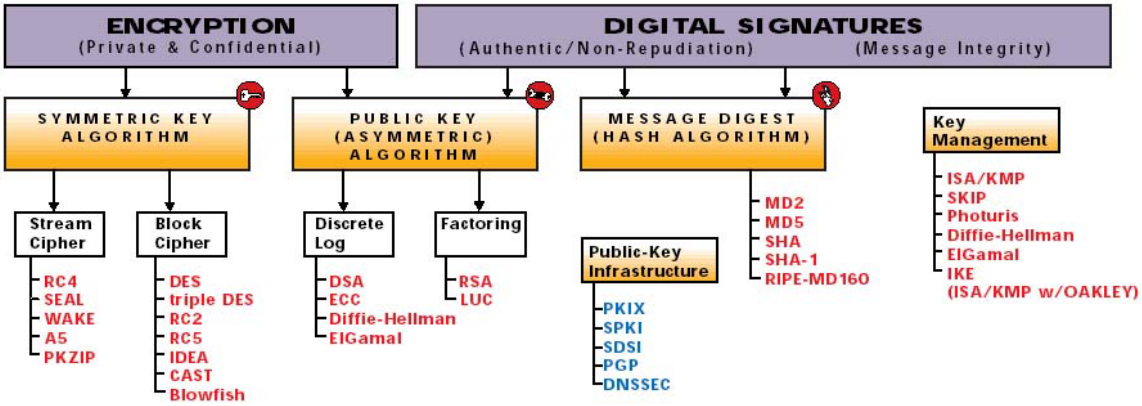
Kriptologija se dijeli na dvije podoblasti: kriptografiju i kriptoanalizu.

Kriptograf traga za metodama obezbjeđenja tajnosti i/ili autentičnosti poruke. **Kriptoanalitičar**,



međutim, nastoji da poništi prethodni posao razbijanjem šifre ili mijenjanjem autentičnosti. Originalna poruka nad kojom kriptograf radi naziva se obično **otvoren tekst** (*Plain Text*), a proizvod njegovog rada naziva se šifrovan tekst ili šifrat. Kriptograf uvijek koristi tajni ključ za kontrolu procesa šifrovanja. On često (ali ne i uvijek) isporučuje tajni ključ nekim od bezbjednijih načina osobi (ili mašini) kojoj će kasnije poslati kriptogram.

Gotovo univerzalna pretpostavka kriptografije je da će neprijateljski kriptoanalitičar imati potpun pristup kriptogramu. Kriptograf se također rukovodi pravilom, koje je prvi uveo naučnik A.Karckhoff (1835-1903), da je bezbjednost šifre sadržana u tajnom ključu. U skladu s tim, Karckhoff-ova pretpostavka je da je čitav mehanizam šifrovanja, izuzev podataka o tajnom ključu, poznat neprijateljskom kriptoanalitičaru. Ako kriptograf usvoji ove dvije pretpostavke, tada on projektuje sistem zaštite od napada na kriptogram. Ako, pak, kriptograf pretpostavi da će se kriptoanalitičar dokopati (milom ili silom) segmenata otvorenog teksta - **kriptograma**, formiranih na osnovu aktuelnog ključa, tada on projektuje sistem zaštite protiv napada na poznat otvoren tekst.



2.5. Kriptouređaji za virtualne privatne mreže (VPN-*Virtual Private Networking*)

2.5.1. Virtuelne privatne mreže (VPN)

Virtuelne privatne mreže su privatne mreže koje su konfigurisane unutar javne mreže. VPN se pojavljuju kao nacionalne ili internacionalne mreže koje , ustvari, dijele glavnu kičmu (*backbone*) sa drugim korisnicima. VPN pospješuju bezbjednost privatnih mreža kontrolom pristupa i šifrovanjem, iskorištavajući upravljanje i pogodnosti izgrađenih velikih javnih mreža.

Vrtoglavi rast Interneta i telekomunikacija, želja za povezivanjem korporacijskih filijala, dovele su do revolucije u poslovnoj komunikaciji. Potreba za razmjenom informacija sa zaposlenima, partnerima i korisnicima širom svijeta, dovele su do razvoja VPN tehnologije preko javnih IP mreža kao što je Internet.

Mnoga preduzeća smanjuju uloženi kapital i operativne troškove oslanjajući svoje mrežne službe na servis provajdere koji mogu ponuditi robusnu, VPN mrežu koja se može proširiti i koja im dozvoljava da se fokusiraju na svoj osnovni posao - zadovoljenje potreba svojih korisnika.

Upravljanje VPN službama uključuje globalnu povezanost za aplikacije vezane za daljinski pristup, intranet i ekstranet, kao i službe za konsalting, dizajn i podršku novih aplikacija, kao što su *Voice over IP*, elektronsku trgovinu i mrežne aplikacije.

Iako se VPN mogu graditi preko ATM-a, *frame relay* i X.25 tehnologija, sadašnji trend je usmjeren ka razvoju IP-VPN mreža. Glavni razlog je taj što beskontaktne IP-VPN mreže nude enormnu fleksibilnost i lakoću u rukovanju. Postavljanjem jednog IP-VPN linka između bilo koje dvije krajnje tačke, bilo gdje u svijetu, samo se zahtijeva konfigurisanje u ovim krajnjim tačkama. IP mreža automatski rukuje rutiranjem saobraćaja između krajnjih tačaka. Pošto ne postoji potreba za prethodnim uspostavljanjem konekcije kroz sve unutrašnje čvorove ili ručno identifikovanje najboljeg puta kroz mrežu, ovo značajno pojednostavljuje planiranje i implementaciju mreže. Pošto su i unutrašnje privatne korporacijske mreže i nove javne VPN službe zasnovane na zajedničkoj IP tehnologiji, investiranje u opremu i trening može biti značajno smanjeno. Kako je Internet dostupan bilo gdje u svijetu, teorijski bilo koja mreža može biti povezana sa drugom mrežom korištenjem IP-VPN tehnologije.

Slijedeća ključna prednost IP-VPN mreža je ta što za razliku od X.25, *frame relay* i ATM službi koje nude kvalitet servisa (QoS) na bazi konekcije, IP-VPN operatori mogu praviti razliku za QoS unutar VPN mreža.

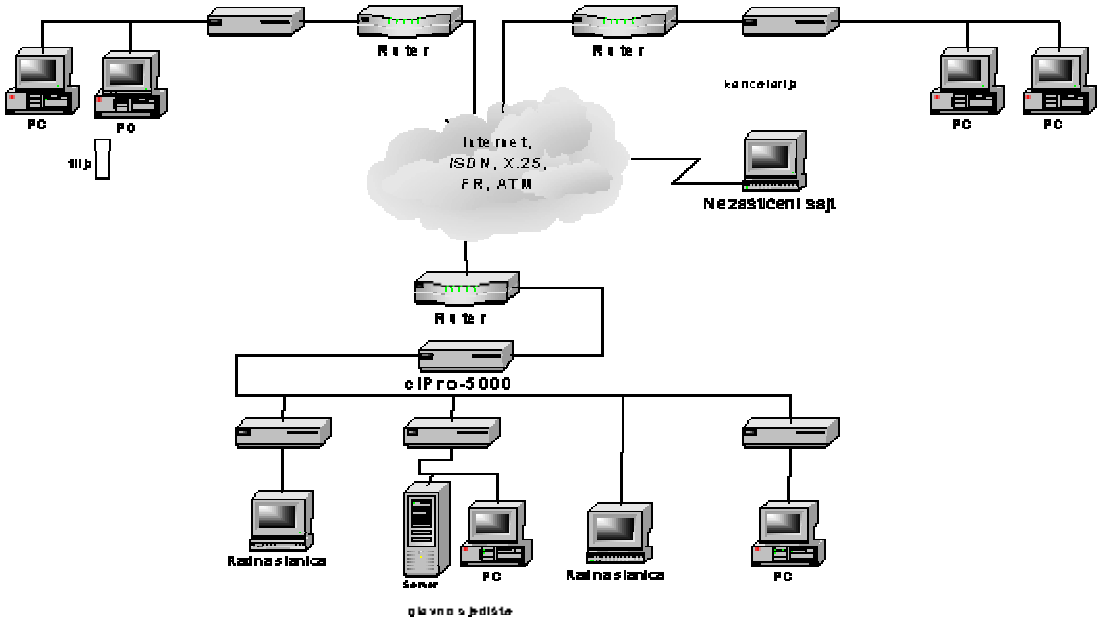
Sposobnost kojom garantuju privatnost i zaštitu podataka je od najveće važnosti kada se razvijaju službe preko Interneta, gdje postoje tačke za ilegalan ulazak koje prijete osjetljivim komunikacijama. Sigurna VPN mreža je komunikaciona mreža koja je obezbijeđena šifrovanjem i autentifikacijom i smještena na postojećim IP mrežama, kao što je Internet, ili kroz mreže provajdera servisa.

Za borbu protiv ugrožavanja mreže, IETF (*Internet Engineering Task Force*) je razvio IP sigurnosni protokol *(IPSec*). Ovaj skup IP ekstenzija koji su zasnovani na modernim kriptografskim tehnologijama nude jaku autentičnost podataka i privatnost garantovanu povećanjem sigurnosti čitave mreže, a ne samo aplikacija. Osnovni IP-VPN sigurnosni servisi uključuju tuneliranje privatnih mreža kroz IP kičmu i šifrovanje podataka. IP-VPN operatori takođe nude centralno upravljanje funkcijama *firewall-a*, sprečavaju neželjeno blokiranje URL-a i *Spam* ili *Junk* e-mail filtriranje.

VPN nude rješenje provajderima servisa i njihovim korisnicima da ojačaju njihovu sposobnost sigurne komunikacije preko daljinskog pristupa i poboljšavaju njihove sveukupne mrežne operacije.

Virtualna privatna mreža se koristi da se omogući međusobno povezivanje klijenata i privatnih mreža preko Interneta, a da se to radi bezbjedno i pored toga što Internet po svojoj prirodi nije bezbjedna mreža. U određenim okolnostima virtualne privatne mreže mogu da obezbijede veze sa udaljenim mrežama, dok u drugom slučaju ove mreže mogu dodatno da uspore već ionako spore komutirane (*dial-up*) mreže.

cIPro-5000 je primjer sveobuhvatnog VPN sistema baziranog na hardveru. Obezbjeđuje šifrovanje visokih mogućnosti i potvrdu vjerodostojnosti uz izuzetnu latentnost, te apsolutnu transparentnost. cIPRo-5000 pruža usluge kriptozaštite naprednim mrežama za sve TCP/IP aplikacije preko svih TCP/IP kičmenih mreža.



Slika 4 - upotreba cIPRo-5000