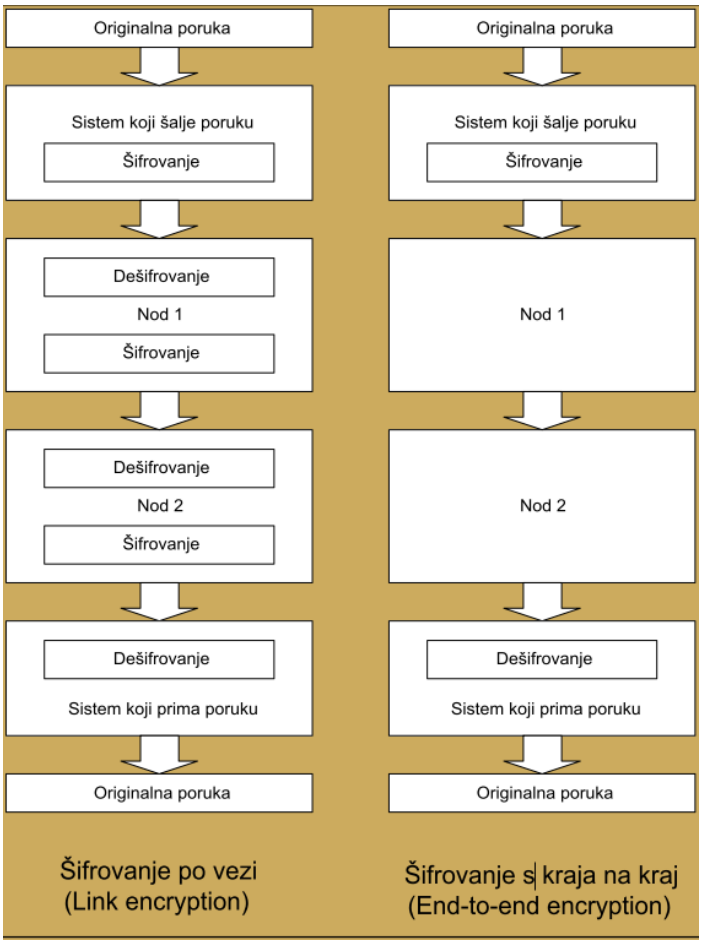
KRIPTOLOŠKA ZAŠTITA U RAČUNARSKIM MREŽAMA

Najvažniji element zaštite podataka u računarskim mrežama predstavlja šifrovanje mrežne komunikacije. Kriptološka zaštita podataka koji se transportuju mrežom može se implementirati na dva načina, slika:

- šifrovanjem sa kraja na kraj (engl. end to end encryption),
- šifrovanjem po vezi (engl. link encryption).

Kod šifrovanja sa kraja na kraj poruka se šifruje pri slanju, a dešifruje po prijemu. Poruka ostaje šifrovana tokom celog putovanja kroz mrežu, od početka do kraja. Kod šifrovanja po vezi poruka se šifruje pri slanju, ali se dešifruje i ponovo šifruje pri svakom prolasku kroz komunikacione čvorove mreže. To znači da se poruka u komunikacionim čvorovima nalazi u nešifrovanom stanju, što predstavlja potencijalnu opasnost.



Slika - Načini za implementaciju kriptološke zaštite u računarskim mrežama

Svaka od pomenutih implementacija ima svoje prednosti i nedostatke. Prednosti šifrovanja sa kraja na kraj su fleksibinost, jednostavna manipulacija i distribucija ključeva za šifrovanje, efikasnost, kao i to što se poruka štiti od početka do kraja komunikacije. Nedostaci se ogledaju u tome MTVU lekciješto neki delovi poruke (npr. zaglavlje poruke i podaci o adresama računara na izvoru i odredištu) moraju da budu u dešifrovanom stanju u toku komunikacije. Prednosti

šifrovanja po vezi su lakoća korišćenja (korisnik ne mora da preduzima bilo kakve akcije) kao i to što se šifruje čitava poruka uključujući i zaglavlje poruke. Osnovni nedostatak šifrovanja po vezi je komplikovana distribucija ključeva za šifrovanje koje mora da poseduje svaki komunikacioni čvor u mreži.

Pored tajnosti komuniciranja kriptografske metode treba da između ostalog obezbede i otkrivanje promena u porukama od strane neovlašćenih osoba, siguran način za distribuciju ključeva za šifrovanje kao i otkrivanje pokušaja napada na mrežu.

SISTEMI ZA ŠIFROVANJE PODATAKA

Moderni šifarski sistemi se mogu klasifikovati u dve grupe:

- Simetrični šifarski sistemi (private key systems),
- Asimetrični šifarski sistemi (public key systems).

Kod simetričnih šifarskih sistema ključ za šifrovanje identičan je ključu za dešifrovanje. Zbog toga se ključ mora tajnim kanalima dostaviti strani koja treba da izvrši dešifrovanje, što ujedno predstavlja jedan od najvažnijih nedostataka ovakvih šifarskih sistema. Simetrični šifarski sistemi nazivaju se još i klasični šifarski sistemi. Sedamdesetih godina prošloga veka dolazi do pojave i naglog razvoja asimetričnih šifarskih sistema kod kojih se ključ za šifrovanje razlikuje od ključa za dešifrovanje i koji su ispravili postojeće nedostatke simetričnih šifarskih sistema.