Predmet: Zaštita informacionih sistema

Profesor: Srđan Maričić

Vezba br. 1

Simetricno sifrovanje i desifrovanje

Drgana Mijailovic

IV-6

Sifrovanje

Sifrovanje (kriptografija) -je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani.

Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje. Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat). Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifru.

Dešifrovanje

Desifrovanje je pretvaranje šifre u otvoreni tekst kad je ključ poznat, vrši ga osoba kojoj je poruka namenjena.

Kriptovanje (Šifrovanje) Simetrično šifrovanje

- Konvencionalno / sa tajnim klju čem / sa jednim klju čem
- Pošiljalac i primalac dele zajednički ključ
- Svi klasi čni algoritmi šifrovanja su zasnovani na tajnom ključu
- Jedini tip šifrovanja do otkri ća javnih klju čeva u sedamdesetim godinama prošlog veka

Kao što smo rekli, kod simetrične enkripcije koriste se isti ključ i za šifrovanje i za dešifrovanje.

Baš zbog toga je raznovrsnost, a samim tim i sigurnost algoritama ovakve enkripcije je velika.

Bitan faktor je i brzina - simetrična enkripcija je veoma brza. Pored svih prednosti koje ima

na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak.

Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi i nju nije potrebno slati drugome).

Klod Šenon je definisao uslove savršene tajnosti, polazeći od sledećih osnovnih pretpostavki:

1. Tajni ključ se koristi samo jednom.
2. Kriptoanalitičar ima pristup samo kriptogramu.

Šifarski sistem ispunjava uslove savršene tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y, što se može matematički izraziti na sledeći način:

$$P(X=x|Y=y)=P(X=x)\}$$

$$P(X=x|Y=y)=P(X=x)\}$$

za sve moguće otvorene tekstove x=(x{1},x{2},...x{m}) x=(x{1},x{2},...x{m}) i sve moguće kriptograme y=(y{1},y{2},...y{n}) y=(y{1},y{2},...y{n}); drugim rečima, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa ili bez poznavanja vrednosti slučajne promenljive Y.

Zbog toga kriptoanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja, nezavisno od raspoloživog vremena i računarskih resursa kojima raspolaže. Koristeći pojam entropije iz teorije informacija, Šenon je odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. Dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M:

$$K \geq M$$

Sekvencijalni šifarski sistemi

Kao najosnovnijim simetričnim algoritmima, dovoljno je samo reći da se oni zasnivaju na svojstvu logičke operacije XOR (engl. exclusive or — ekskluzivno ili) za koju vazi:

$(X \text{ xor } Y) \text{ xor } Y = X,\ X, Y \in (0,1)$

Naime, možemo zamisliti da nam je X jedan bit originalne poruke a Y bit ključa. Tada (X xor Y)=Z predstavlja jedan bit šifrata koji putuje javnim kanalima i koji neko može prisluškivati, dok je Z xor Y originalni bit X koji se dobija xor-ovanjem bita kodirane poruke sa bitom ključa. Definišimo još operaciju xor za proizvoljnu dužinu bita tj. bajtova i tada X, odnosno Y možemo smatrati bajtom, rečju odnosno porukom U praksi se često koriste generatori pseudo slučajnih nizova (engl. PRNG – Pseudo Random Number Generator), koji predstavljaju determinističke algoritme za

šifrovanje, ali nizovi simbola koje oni generišu imaju osobine slične slučajnim nizovima. Generatori pseudoslučajnih nizova koriste kratke ključeve radi započinjanja procesa generisanja. Ovi ključevi moraju biti prisutni na obe strane pre početka komuniciranja. Izlazni niz iz generatora se sabira po modulu 2 sa nizom otvorenog teksta i na taj način se dobija niz šifrata. Na prijemnoj strani se sabira primljeni niz šifrata sa pseudoslučajnim nizom generisanim pomoću istog ključa, počevši od istog početnog simbola kao i na predajnoj strani. Na taj način je prijemnik u stanju da rekonstruiše otvoreni tekst. Jasno je da dokle god se slučajni nizovi dobijaju pomoću bilo kog algoritma oni mogu biti samo pseudoslučajni i kao takvi postaju mamac za sve one koji se bave razbijanjem šifri. Pseudoslučajni nizovi su periodični u širem smislu (što znači da mogu imati aperiodični početak), ali ako su periodi takvih nizova mnogo veći od dužina nizova otvorenog

teksta, sistem će se ponašati na sličan način kao i Vernamova šifra. Osnovna ideja koja stoji iza sekvencijalnih šifara je da se generiše duga i nepredvidljiva sekvenca simbola iz nekog alfabeta (npr. binarnog) na osnovu kratkog ključa izabranog na slučajan način. Sekvencijalna šifra sa generatorom pseudoslučajnog niza je aproksimacija Vernamove šifre, i utoliko je bolja ukoliko je pseudoslučajni niz bliži po karakteristikama pravom slučajnom nizu.

Blok šifra

Blok šifrom se nazivaju oni algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima) od dva i više elemenata. Najpoznatiji algoritmi blok šifara su: LUCIFER, DES, FEAL, IDEA, RC5, SKIPJACK, BLOWFISH, TWOFISH, AES (RIJNDAEL) i drugi.