Kriptoanaliza simetričnih algoritama

Vrsta: Seminarski | Broj strana: 17 | Nivo: Visoka tehnička škola strukovnih studija Kragujevac

Sadržaj

Uvod

Kriptoanaliza (od grčkog kryptós (skriveno) i analýein (razmrsiti)) predstavlja proučavanje metoda za saznavanje šifrovanih informacija, bez posedovanja tajnih podataka koji su obično potrebni da bi se pristupilo tim informacijama. Ovo obično podrazumeva pronalaženje tajnog ključa. Netehničkim izrazima, kriptoanaliza je praksa razbijanja šifara, mada ovaj izraz ima specijalizovano tehničko značenje.

Kriptoanaliza se takođe koristi da označi svaki pokušaj zaobilaženja drugih tipova kriptografskih algoritama i protokola uopšteno. Međutim, kriptoanaliza obično ne razmatra metode napada čija primarna meta nisu slabosti posmatranog kriptografskog sistema, kao što su potplaćivanje, fizička sila, provaljivanje, logovanje tastature, ili socijalno inženjerstvo, mada ovi tipovi napada jesu važna stavka, i češće dovode do rezultata nego tradicionalna kriptoanaliza.

Iako je cilj oduvek isti, metode i tehnike kriptoanalize su se tokom istorije kriptografije drastično promenile, prilagođavajući se povećanoj kompleksnosti kriptografije, počev od metoda koji su podrazumevali papir i olovku, preko mašina kao što je Enigma tokom Drugog svetskog rata, do računarski baziranih napada današnjice. Sredinom sedamdesetih godina dvadesetog veka je uvedena nova klasa kriptografije: asimetrična kriptografija. Metodi za razbijanje ovih kriptosistema su obično radikalno drugačiji nego ranije, i obično podrazumevaju rešavanje pažljivo konstruisanih problema iz čiste matematike, među kojima je je najpoznatiji faktorizacija celih brojeva.

Cezarov enkripcioni metod

Ciphertext-only attack je dostupan za Cezarov algoritam u formi automatske pretrage ključa.

U analizi, računa se frekvencija ponavljanja svakog karaktera I kao rezultat dobija se histogram. Frekvencija ponavljanja pojedinačnih karaktera se upoređuje sa frekvencijom ponavljanja karaktera u engleskom jeziku. Ovo podrazumeva predpostavljanje raspodele sa različitim offsetovima i poređenje njihovih frekvencija ponavljanja. Offset sa najviše sličnosti sa frekvencijom raspodele engleskog jezika se uzima kao tačan ključ. U dialogu Opcije za atomatsku analizu moguće je odrediti koji i koliko međurezultata obrade će biti prikazani u posebnim prozorima. Ukoliko korisnik klikne na Cancel umesto Ok dok gleda neki od ovih međurezultata obrade, ni jedan od ovih prozora se više neće prikazati. Ključ koji je CrypTool koristio prikazan je u dijalogu Automatske analize. Takođe može biti zamenjen u ovom istom dialogu.

Primer:

Za potrebe ovog primera potrebno je da nam budu otvorena dva prozora(slika 1(tekst koji se šifruje) i slika 2(šifrovani tekst)).

Slika 1.

Slika 2.

Prvo, moramo postaviti prozor koji sadrži tekst koji se šifruje da bude aktivan. Sada možemo doći do podataka o ovom tekstu i to preko funkcije Entropy koja nam pokazujem broj različitih karaktera koji se koriste u tekstu i do frekvencije ponavljanja određenih karaktera, koja se dobija korišćenjem funkcije histogram (slika 3.)

...