SIMETRIČNI I ASIMETRIČNI ŠIFARSKI SISTEMI

SIMETRIČNI ŠIFARSKI SISTEMI

Simetrični šifarski sistemi karakterišu se relativno velikom brzinom rada i jednostavnom implementacijom. Mogu da obezbede kvalitetnu zaštitu komunikacionih kanala u računarskim mrežama pod uslovom da se tajni ključ za proces šifrovanja, odnosno dešifrovanja transportuje sigurnim kanalima i da je nepoznat potencijalnim napadačima.

Zahtevi za tajnošću i autentičnošću kod simetričnih šifarskih sistema zasnivaju se upravo na tajnosti ključa. Ukoliko napadač ne poseduje tajni ključ, on nije u mogućnosti da otkrije sadržaj poruke. Zbog ove činjenice MTVU lekcijenajveći problem kod simetričnih šifarskih sistema je upravo obezbeđivanje sigurnih kanala za distribuciju tajnih ključeva.

DES ("Federal Data Encryption Standard") je jedan od najpoznatijih simetričnih sistema za šifrovanje. Iako je 1977. godine data preporuka od Američkog nacionalnog biroa za standarde za korišćenje ovog sistema, vlada SAD nikada nije koristila DES za zaštitu svojih poverljivih podataka zbog toga što je dužina ključa od 56 bita dovoljno kratka za pokušaje brute force napada.

U novije vreme od simetričnih sistema za šifrovanje izdvojio se tzv. IDEA (International Data Encryption Algorithm) algoritam koji koristi ključ od 128 bita i koji je dosta brži u softverskoj implementaciji od DES algoritma. Razvijen je u Cirihu od strane James L. Masseya i Xuejia Laia, a objavljen je 1990 godine. Do sada je IDEA algoritam bio otporan na različite pokušaje dekriptovanja, a najnoviji dokazi ukazuju na to da je IDEA algoritam otporniji od DES algoritma.

ASIMETRIČNI ŠIFARSKI SISTEMI

Sedamdesetih godina prošloga veka učinjen je veliki napredak u kriptografiji sa pojavom asimetričnih šifarskih sistema koji se još nazivaju i sistemi javnih ključeva (engl. public key systems). Do tada su se koristili samo simetrični šifarski sistemi koji se zbog toga i nazivaju konvencionalnim sistemima za šifrovanje.

Asimetrični šifarski sistemi rešili su dva velika problema simetričnih šifarskih sistema, a to problem distribucije tajnih ključeva i problem autentifikacije poruka.
Kod asimetričnih sistema postoje dva ključa. Jedan za šifrovanje a drugi za dešifrovanje. Ključevi nisu isti ali su povezani jedan sa drugim određenim transformacijama. Poznavanje jednog ključa i algoritma transformacije ne omogućava dobijanje drugog ključa. Jedan od ključeva se označava za javni (eng. public key) i može se slobodno distribuirati, dok se drugi označava kao tajni i mora biti dostupan samo njegovom vlasniku. Javni ključ se obično koristi za šifrovanje poruka koje se upućuju njegovom vlasniku. Ovakve poruke može dešifrovati samo vlasnik odgovarajućeg tajnog ključa. Na taj način moguće je izvršiti šifrovanje, ali ne i dešifrovanje poruke.

Pri distribuciji javnih ključeva treba voditi računa da može doći do zloupotrebe istih zbog neodgovarajuće autentifikacije. Naime, ukoliko MTVU lekcijekorisnik A pošalje svoj javni ključ korisniku B, a korisnik C presretne tu komunikaciju i zameni javni ključ korisnika A svojim javnim ključem koji dalje prosledi korisniku B, tada će on biti u stanju da pročita svaku poruku korisnika B korisniku A. No, to nije sve. Korisnik C će dalje moći da dešifrovanu poruku šifruje uz pomoć

originalnog javnog ključa korisnika A i predstavljajući se kao korisnik B pošalje šifrovanu poruku korisniku A. Sigurno najpoznatijiasimetrični algoritam za šifrovanje je svakako RSA (Rivest-Shamir-Adleman). Ovaj algoritam implementiran je u program za šifrovanje PGP (Pretty Good Privacy) autora Philipa Zimmermanna koji se najčešće koristi za ostvarivanje sigurnosti elektronske pošte (engl. e-mail) u računarskim mrežama. PGP obezbeđuje autentifikaciju, digitalni potpis šifrovane poruke, kompresiju korišćenjem ZIP algoritma i radix 64 konverziju binarnih datoteka u ASCII radi slanja putem elektronske pošte.

PGP omogućava i biranje veličine javnih i tajnih ključeva koja može biti: obična (384 bita), komercijalna (512 bita) i vojna (1024 bita). PGP šifruje poruku korišćenjem IDEA algoritma ključem od 128 bita koji se kreira na slučajan način prilikom šifrovanja. Ovaj ključ se dalje šifruje uz pomoć RSA algoritma i šalje zajedno sa šifrovanom porukom. PGP takođe kreira digitalni potpis na osnovu sadržaja poruke uz pomoć MD5 algoritma a dobijena vrednost se šifruje RSA algoritmom. Ovakav sistem šifrovanja izveden je da bi se izbeglo šifrovanje cele poruke RSA algoritmom koji je veoma spor.

DIGITALNI POTPIS

Digitalni potpis odgovara fizičkom potpisu pisanog dokumenta i primenjuje se da bi se nedvosmisleno garantovao identitet kreatora poruke. Digitalni potpis treba između ostalog da omogućava verifikaciju autora i vremena potpisa kao i jednostavno kreiranje, prepoznavanje i proveru potpisa. Zlonamerno menjanje potpisa bez mogućnosti otkrivanja mora biti vremenski neisplativo.

Digitalni potpis mora biti različit pri svakom procesu potpisivanja. Da bi se ovaj zahtev ispunio, digitalni potpis se postavlja kao funkcija poruke koja se potpisuje. U transformaciju se mogu uključiti i parametri kao što su vreme potpisivanja i sl.

Digitalni potpisi se obično generišu uz pomoć različitih "hash" funkcija i korišćenjem asimetričnih šifarskih sistema kao što je RSA. Kriptološka "hash" funkcija na ireverzibilan i poznat način od poruke MTVU lekcijeproizvoljne dužine stvara zapis fiksne dužine (obično 512 bita) koji u potpunosti odslikava sadržaj poruke tako da svaka promena u sadržaju poruke utiče na promenu potpisa.