O šifriranju podatkov

Osnovni pojmi in nekaj primerov

Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Beseda
prihaja iz grščine: kryptos logos pomeni skrita beseda. Uporabljata se še pojma enkripcija (šifriranje) in dekripcija. Osnovno sporočilo
ponavadi imenujemo čistopis (cleartext, plaintext), zašifrirano pa šifropis ali tajnopis(kriptogram, ciphertext)

Sporočilo po nekem postopku (algoritmu, metodi) spremenimo v kriptirano sporočilo, pri tem uporabimo določene vrednosti za
parametre v algoritmu, ki jim rečemo ključ. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana
sporočila. V zgodovini je bilo razvitih nešteto metod, pa tudi literature o tem je veliko, že celo v slovenščini.

Primeri

Špartanci so uporabljali naslednji način: na valj so navili ozek trak in sporočilo napisali pravokotno na smer traku. Poslali so odvit trak,
naslovnik pa je moral imeti valj enakega premera.

Julij Cezar je svojim vojskovodjem pošiljal sporočila, kjer je vsako črko zamenjal s črko, ki je bila v abecedi nekaj mest za njo.
Postopek lahko opišemo kot zamenjavo črk a -> a+k po modulu 25 (tu smo metodo priredili za slovensko abecedo s 25 črkami). "k"
predstavlja ključ. Cezar je menda običajno uporabil ključ 3. Kako bi dešifrirali HAL, če vemo, da smo uporabili isti algoritem s ključem
-1?

Do pred nedavnim je bil v uporabi postopek ROT-13 (zamenjava črk a -> a+13 po modulu 26 - angleška abeceda) v Usenetu za
šifriranje neprimernih šal in podobnega. Seveda ni predstavljal nobene resne zaščite. Netscape-ov brkljalnik je imel v prvih verzijah
vgrajeno možnost pod View -> Unscramble ROT-13.

Tudi pri opisu sodobnih algoritmov bomo naleteli na izraz a b mod m , kar beremo "a je kongruentno b po modulu m". Ta izraz
velja, kadar je a - b mnogokratnik m, torej kadar sta števili a in b na številski premici med seboj oddaljeni za mnogokratnik od m. V
sodobnih metodah so velikokrat uporabili izreke iz kongruenčne aritmetike.

7 17, 27, 37,..., -3, -13, ... po modulu 10.

Enigma- šifrirni stroj, ki so ga uporabljali Nemci med 2.svetovno vojno

Vse doslej naštete algoritme imenujemo simetrični algoritmi ali algoritmi s privatnim ključem: imamo samo en ključ, s katerim
zašifriramo in dešifriramo sporočilo.

šifriranje s simetričnimi algoritmi je običajno hitro, težko pa je varno izmenjati ključ. Problem predstavlja tudi število ključev - vsak
uporabnik mora imeti za vsakega dopisovalca svojega.

Ravno zaradi teh problemov so se razvile asimetrične metode ali algoritmi z javnim ključem (začetki v letu 1975). Uporabnik si

skreira dva ključa in enega objavi. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral
pa ga bo lahko le on sam, ki pozna še svoj skriti ključ. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.

Pri pošiljanju sporočila po internetu ni dovolj, da sporočilo zašifriramo. Ko potuje po javnih vodih, preko nešteto vozlišč, lahko kdo naše
zašifrirano sporočilo spremeni. Pojavi se tudi problem identifikacije lastnika javnega ključa - ali ni objavil ključa namesto mene kdo drug,
ki se hoče izdajati za mene in dobivati pošto, namenjeno meni. Varnostna aplikacija mora torej zagotoviti naslednje:

- zaupnost (confidentiality);
- celovitost (integrity);
- overjanje (authentication);
- preprečevanje tajenja (nonrepudiation);
- kontrolo dostopa (access control).

Zato se je razvilo podpisovanje sporočil (digital signitures) in certificiranje ključev. Certifikat vsebuje poleg podatkov o ključu še
čas nastanka, podatke o lastniku, rok veljavnosti ipd.

V aplikacijah, ki omogočajo zaupnost pošiljanja sporočil, se uporablja obe vrsti algoritmov. Obenem vključujejo zgostitvene algoritme,
ki poljubno dolg tekst preslikajo v število fiksne dolžine (npr. 128 bitov). Najbolj znana sta MD5 in SHA. Poleg tega pred šifriranjem
tekst običajno stisnemo na manj kot polovico dolžine z enim od programskih produktov za to. Vhod v kriptografske algoritme predstavlja
binarni zapis.

Če hočemo zagotoviti verodostojnost svojega sporočila, mu dodamo digitalni podpis: z zgostitvenim algoritmom izračunamo fiksni
"povzetek" sporočila, ki ga zašifriramo s svojim privatnim ključem. Prejemnik bo najprej z našim javnim ključem dešifriral podpis, iz
sporočila bo ponovno izračunal povzetek ter ga primerjal s tistim, ki ga je dobil v podpisu. Če se ujemata, je dobil tako sporočilo, kot
smo ga podpisali.

Ker se s kriptologijo ukvarja veliko institucij z močnimi ekipami, je razumljivo, da so danes varnejši znani, javno objavljeni in
preizkušeni algoritmi, pri katerih je vsa tajnost zagotovljena s ključem. Čim daljši je ključ, teže ga je razkriti. Ključi pri asimetričnih
metodah morajo biti daljši od simetričnih za isto stopnjo varnosti. Ocenjujejo, da ključu simetrične metode dolžine 56 bitov ustreza javni
ključ 384 bitov (in 128 bitov : 2304 bitov). V splošnem svarijo pred nakupom šifrirnih naprav, če prodajalec noče objaviti algoritma
šifriranja. Ameriški produkti imajo zaradi izvoznih omejitev za neameriške kupce skrajšane ključe ali pa nudijo šibkejše algoritme. O tem
govori dokument z zanimivim naslovom Snake Oil FAQ.

Zdaj smo si ogledali algoritme, ki jih uporabljamo pri šifriranju: simetrične , asimetrične in zgostitvene. Za šifriranje podatkov vedno
uporabljamo simetrične algoritme, ker so hitrejši od asimetričnih. Vendar moramo pred tem izmenjati ključ za simetrični algoritem. To
lahko naredimo tako, da se priključimo na nek centralni strežnik ključev ali pa uporabimo asimetrični algoritem. V protokolih SSL,
IPSEC in SET uporabimo asimetrični algoritem za izmenjavo skupnega skritega ključa.

Šifriranje lahko vključimo v katerikoli komunikacijski sloj:

Šifriranju na najnižjih slojih rečemo link-by-link šifriranje. Na ta način povsem zaščitimo pot med dvema napravama, zašifrirana je vsa
informacija na višjih nivojih, tudi IP številke. Zato je treba na vseh vmesnih postajah izvesti dešifriranje. Šifriranje je on-line. Ta način je
primeren za vojsko ali pa banke, kjer gre za povezave med točno določenimi postajami, ki jih opremimo s šifrirnimi napravami.

Šifriranju na višjih slojih rečemo end-to-end, ker IP številke niso zašifrirane in usmerjevalniki lahko usmerjajo pakete zašifrirane.Dešifrira
se samo na končni postaji. Slaba stran tega je, da lahko nasprotnik dela analizo prometa med posameznimi vozli. Imamo pa možnost
izmenjevati podatke med različnimi postajami in mrežami (tudi po internetu), če so opremljene z interoperabilno opremo za šifriranje. Če
šifriranje in overjanje vključimo v omrežni sloj, je zaščiten ves promet in aplikacijam ni treba skrbeti za to. To pa ni vedno dobro, saj
šifriranje upočasni prenos, poleg tega lahko komunicirajo samo naprave s kompatibilno šifrirno opremo. Zato je včasih bolje, da za
šifriranje poskrbi aplikacija, kjer je tudi lažje overoviti posamezne uporabnike.

Zdaj si oglejmo nekaj načinov uporabe šifriranja podatkov. Protokol IPSEC bo vključen v novo verzijo protokola IP (IPV6), je pa že
zdaj precej v uporabi. Zašifrirano je vse razen IP številke.

Na aplikacijskem nivoju:

Za elektronsko pošto je narejenih že kar nekaj aplikacij, kjer uporabnik lahko poskrbi, da je sporočilo zašifrirano. Najbolj znana je PGP
(Pretty Good Privacy), kjer je digitalni podpis narejen z uporabo RSA in MD5, sporočilo pa se zašifrira z uporabo algoritma IDEA in
sicer s ključem seje, le-tega pa zašifriramo z RSA.

Tudi za www se pojavljajo zanimive rešitve, ki avtomatično zašifrirajo podatke, preverijo avtentičnost strežnika itd. Zaenkrat so
najpogosteje omenjeni:

- SSL (Secure Sockets Layer),, ki ga razvija Netscape,
- PCT (Private Communication Technology) - Microsoft, ki je na srečo soroden SSL,
- TLS (Transport Layer Security) - protokol, ki ga na osnovi SSL pripravlja IETF
- S-HTTP (Secure HTTP) - Terisa Systems.

Četrta rešitev protokolu HTTP dodaja možnost, da se datoteke izmenjujejo zašifrirane(predlog protokola). Prva rešitev in naslednji dve,
ki sta izpeljani iz nje, pa so zamišljene tako, da med transportni (TCP) in aplikacijski nivo dodamo nov protokol za šifriranje prometa
med strežnikom in odjemalcem - tako je možno zaščititi vse aplikacije nad tem nivojem (http, telnet, ftp, news). S-HTTP skoraj ni več v uporabi - težko najdemo strežnik ali brkljalnik, ki ga še podpira - SSL je postal de facto standard.

Tudi bančne organizacije, ki izdajajo kreditne kartice, želijo izkoristiti internet za poslovanje. Tako Visa in Mastercard skupaj z drugimi
izdajatelji kreditnih kartic razvijajo in testirajo protokol SET (Secure Electronic Transaction) za podporo nakupovanju s kreditnimi
karticami.

URL: http://www.sigov.si/tecaj/kripto/kr-osn.htm