Tečaj o internetu

O šifriranju podatkov

Algoritmi z javnim ključem

Naloga, najti način šifriranja podatkov, kjer bosta znana metoda in ključ za šifriranje, pa vendar bo podatke lahko dešifriral samo
naslovnik, se zdi težko uresničljiva. Najti je treba tako transformacijo, za katero je težko ali nemogoče izvesti inverzno transformacijo, če
nimamo dodatne informacije (privatnega ključa). Za take transformacije se uporablja izraz One-Way Function oziroma Trap-door
one-way function: inverzna operacija je lahka, če imamo neko dodatno informacijo (trap-door), sicer pa skoraj nemogoča.

Koncept javnega ključa sta prva predstavila Whitfield Diffie in Martin Hellman (1975) - The Diffie-Hellman key agreement protocol.
To ni algoritem za šifriranje podatkov, temveč postopek za kreiranje in izmenjavo skritega ključa po javnem omrežju.

Imamo parametra p in g, ki sta oba javno znana. p je praštevilo, g (generator) pa celo število, manjše od p, iz katerega lahko
dobimo katerokoli število od 1 do p-1, če ga potenciramo in vzamemo vrednost po modulu p.

Alica si izbere naključno število a, Bob pa svojega (b). Potem Alica izračuna svoj javni ključ ga mod p, Bob pa svojega gb mod
p. Ti števili si izmenjata. Njun skrivni ključ Alica izračuna takole: kab (gb)a mod p, Bob pa poišče vrednost kba (ga)b mod
p. Ker je kab = kba , imata skupni skrivni ključ, ki ga lahko uporabita kot ključ za šifriranje podatkov s katerim od simetričnih
algoritmov.

Če je praštevilo p dovolj veliko, je skoraj nemogoče izračunati gab mod p iz ga mod p in gb mod p.

Na podobnih osnovah temelji algoritem ElGamal, ki se v glavnem uporablja za digitalno podpisovanje.

Prvi znani algoritem z javnim ključem za šifriranje podatkov je Merkle-Hellmanova metoda z nahrbtniki, vendar ni več v uporabi.

Danes se najbolj uporablja algoritem RSA, ki ima ime po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman) - MIT, 1977.
Metoda je v ZDA patentirana. Ker pa je bil opis metode objavljen pred vložitvijo zahtevka za patent, lahko RSA uporabljajo brez
licenčnine povsod v svetu, razen v ZDA.

Metoda temelji na dejstvu, da je razmeroma lahko najti dve veliki praštevili, če pa poznamo samo njun zmnožek, je težko najti faktorja.
Vzemimo primer s 3-številčnima praštevilom: 191 x 283 = 54053. Če hočemo faktorirati to število, se bomo kar nekaj časa trudili. V
praksi pa so ta števila 70 in več številčna.

Osnovo metode prestavlja naslednji izrek iz kongruenčne aritmetike, ki ga pripisujejo Eulerju:
Naj bosta p in q različni praštevili, velja naj tudi ed 1 mod (p-1)(q-1).

Potem sledi (Te)d T mod pq.

Če nam T predstavlja blok teksta, ga zašifriramo takole: s Te mod pq
dešifriramo pa: T sd mod pq.
Če označimo n = pq, javni ključ sestavljata n ter e, skriti ključ pa p, q in d.

Kako bomo izbrali vrednosti p, q, e in d? p in q morata biti veliki praštevili- več sto-mestni števili, razmeroma blizu skupaj. V praksi
za e običajno izberemo 3 ali 65537 (216+1). Zdaj izračunamo produkt (p-1)(q-1). Drugo predpostavko iz gornjega izreka lahko
izrazimo tudi takole:
ed -1 je deljivo s (p-1)(q-1) oziroma v obliki Diofantske enačbe: ed + k(p-1)(q-1) = 1. Ta pa je rešljiva s celimi števili, če velja, da
sta števili e in d tuji proti p-1 in q-1 (nimajo skupnih deliteljev). Izberemo tako število, ki je večje od p+1 oziroma q+1 in manjše od
produkta (p-1)(q-1). Zdaj izračunamo število d iz formule ed mod (p-1)(q-1) 1.

Sporočilo, ki ga želimo šifrirati, najprej razbijemo na bloke, krajše od pq, - danes je to ponavadi 512 ali 1024 bitov. Izračunamo
vrednost s Te mod pq za vsak kos sporočila. Ta števila združimo in dobimo šifrirano sporočilo. Pri dešifriranju spet najprej
razbijemo sporočilo na bloke in na vsakem uporabimo formulo T sd mod pq.

Za ponazoritev naredimo primer za majhna števila.

Vohun bi moral najprej najti števili p in q iz njunega produkta, to pa je po sedaj znanih metodah pri velikih p in q dolgotrajen
postopek. Znan je naslednji primer:
Martin Gardner je avgusta 77 objavil v Scientific Americanu 129 številk dolgo število in ponudil 100 dolarjev za razbitje na
faktorje. Uganko je rešila mednarodna skupina iz več kot 600 prostovoljcev jeseni 1994.

Na voljo je veliko komercialnih izvedb RSA (tako softverskih kot hardverskih). Uporabljajo se ključi (s tem mislimo produkt pq) daljši
od 512 bitov. Za ameriške firme velja omejitev za izvoz: dobiti morajo dovoljenje vlade, ta pa običajno ne dovoli izvoziti programa, ki
uporablja daljši ključ od 512 bitov. RSA Laboratories priporoča ključ 768 bitov za osebno uporabo, 1024 bitov za uporabo v
organizacijah in 2048 bitov za ključe v izredno pomembnih operacijah.

Zadnje čase je veliko govora o asimetričnih algoritmih, ki temeljijo na eliptičnih krivuljah (ECC - elliptic curve cryptosystems). Ideja je
znana že od leta 1985. Najdlje na tem področju je kanadska firma Certicom. V primerjavi z RSA zadoščajo krajši ključi, zato kaže, da
bodo v bodočnosti ti algoritmi prevladali.

dolžina ključa ECC	dolžina ključa RSA
106 bitov	512 bitov
132 bitov	768 bitov
160 bitov	1024 bitov
191 bitov	1536 bitov
211 bitov	2048 bitov

Asimetrični algoritmi se uporabljajo za izmenjavo skupnih ključev in za digitalno podpisovanje, za masovno šifriranje
podatkov pa ne, ker so počasnejši od simetričnih algoritmov.

ime	matematična osnova	namen	uporaba
Diffie-Hellman	diskretni algoritmi	izmenjava skritega ključa	v protokolih IPSEC, SSL, ...
ElGamal	diskretni algoritmi	digitalen podpis, enkripcija	za digitalen podpis v DSS
RSA	faktoriranje velikih števil	digitalen podpis, enkripcija	zaenkrat najbolj pogosto uporabljen asim.algoritem
ECC	eliptične funkcije	digitalen podpis, enkripcija	naslednik RSA ?

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