Kriptografija

Jan Malec, Gimnazija Koper
Lara Kavčič, Gimnazija Koper
Žiga Gregorin, Gimnazija Velenje
Maruša Pečovnik, I. gimnazija v Celju
Mentorica: Maja Alif, UL FMF

Beseda kriptografija izhaja iz grških besed *kryptos* (skrit) in *graphein* (pisati). Ta znanstvena disciplina proučuje teoretične in praktične vidike skrivanja sporočil. Povezuje področja matematike, računalništva in elektrotehnike. Da so algoritmi kar se da učinkoviti, jih pogosto prevedemo v matematični jezik, saj jih tako lažje analiziramo. Brez uporabe računalnika si kriptografijo danes težko predstavljamo. Šifriranje na roke je zastarelo, prepočasno in neučinkovito. Elektrotehnika pa priskrbi strojno opremo, kjer je algoritme možno zares implementirati.

Kriptografija igra pomembno vlogo v človeški zgodovini. Sporočila je bilo vedno potrebno skrivati pred sovražnikovim pogledom, zato se je šifriranje še posebej razmahnilo v negotovih vojnih časih. To je prineslo marsikaj koristnega tudi za širšo družbo v povojnih časih. Med drugo svetovno vojno so bili v uporabi zelo sofisticirani sistemi (npr. nemška enigma), ki so od nasprotnikov zahtevali veliko znanja in iznajdljivosti, če so hoteli prestreči sporočilo in pričakati napadalce. V Veliki Britaniji se je Alanu Turingu porodila ideja o Turingovem stroju, predhodniku današnjih računalnikov.

1 Klasična kriptografija

Stari Grki in Rimljani so poznali že veliko dobrih načinov šifriranja, ki pa se danes ne uporabljajo več, saj se jih da z računalniki enostavno razbiti. To so bili simetrični kriptosistemi, kar pomeni, da je ključ za šifriranje in dešifriranje enak.

1.1 Cezarjeva šifra

Cezarjeva šifra je dobila ime po znanem rimskem cesarju Juliju Cezarju, ki jo je uporabljal za pošiljanje vojaških sporočil. Vsaki črki abecede priredimo določeno število (A $\to$ 0, B $\to$ 1 $\ldots$ Ž $\to$ 24). Kodiranje poteka tako, da najprej na ta način spremenimo besedilo in mu prištejemo neko izbrano število n, ki ga imenujemo *ključ*.

Zgled 1. Zakodirajmo s ključem $n = 4$ besedo *šifra*. Najprej črkam priredimo številke, in jim nato prištejemo n.

19	9	6	17	1
Š	I	F	R	A

$$\Downarrow$$

23	13	10	21	5
Z	M	J	U	E

Za dekodiranje uporabimo isti ključ, le da je operacija odštevanje.

1.2 Substitucijska šifra

Pri substitucijski šifri črke abecede zamenjamo med seboj. Poznamo tudi *substitucijske šifre s ključno besedo*, pri kateri besedilo razdelimo na bloke enake dolžine kot je ključna beseda. Prvi črki besedila prištejemo prvo črko ključne besede, drugi drugo itd.

Zgled 2. Naj bo ključna beseda *šifra*, zakodirajmo pa *ponedeljek*.

19	9	6	17	1	19	9	6	17	1
Š	I	F	R	A	Š	I	F	R	A

16	15	14	6	5	6	12	10	6	11
P	O	N	E	D	E	L	J	E	K

$$\Downarrow$$

11	24	20	23	6	1	21	16	23	12
K	Ž	T	Z	E	A	U	P	Z	L

Postopek za dekodiranje je enak, le da ključno besedo "odštevamo".

1.3 Permutacijska šifra

Pri tem postopku uporabimo na besedilu permutacijo dolžine n. Razdelimo ga na bloke, dolge n znakov, in v vsakem bloku premešamo črke, kot to določa ključ – izbrana permutacija. Danes se ta šifra še vedno uporablja, a le kot del kakšne kompleksnejše.

2 Moderna kriptografija

V dobi računalnikov temelji varnost kriptosistemov na težkih matematičnih problemih.

2.1 Kongruence

Izberimo si $a, b \in \mathbb{Z}$ in število m, ki naj bo neničelno in celo. Če dasta števili a in b pri deljenju z m enak ostanek, oziroma če m deli razliko $a - b$ pravimo, da sta a in b *kongruentni* po modulu m. To označujemo

$$a \equiv b \mod m.$$

V nadaljevanju bomo brez dokazov predstavili še dva pomembnejša izreka.

Izrek 1 (Mali Fermatov izrek)**.** *Naj bo p praštevilo in a naravno število, tuje proti p. Tedaj velja:*

$$a^{p-1} \equiv 1 \mod p.$$

Izrek 2. *Naj bo $n \in \mathbb{N}$ oblike $p \cdot q$, kjer sta p in q praštevili. Naravno število a naj bo tuje proti n. Tedaj velja*

$$a^{(p-1)(q-1)} \equiv 1 \mod n.$$

2.2 RSA

RSA je novodobni sistem za šifriranje sporočil, ki temelji na praštevilih. Leta 1978 so ga javno opisali ameriški znanstveniki (vsi z MIT): Ron Rivest, Adi Shamir in Leonard Adleman. Ime algoritma je sestavljeno iz začetnic njihovih priimkov, v vrstnem redu kot so bili podpisani v članku.

1. Najprej določimo ključ.
   (a) Naključno si izberemo dve praštevili, ki morata imeti približno enako število števk. Imenujemo ju p in q, njun zmnožek pa je n.
   (b) Potem izračunamo $m = (p - 1)(q - 1)$.
   (c) Izberemo si poljubno število e, za katerega mora veljati: $1 < e < m$ in e je tuj proti m. Število e je *javni del ključa*, ki ga lahko vidijo vsi in ga morajo poznati, da nam lahko pošljejo sporočilo.

(d) *Zasebni del ključa* je število d, ki ga izračunamo iz enačbe: $de \equiv 1 \mod m$.

2. Naj bo x sporočilo (že v številkah). Kriptogram c dobimo s kodirno funkcijo:

$$c \equiv x^e \mod n.$$

3. Za dešifriranje uporabimo zasebni ključ d. Originalno sporočilo izračunamo s pomočjo dekodirne funkcije:

$$x \equiv c^d \mod n.$$

Na prvi pogled ni jasno, da nam ta postopek res dekodira originalno sporočilo, zato predstavimo še dokaz.

Dokaz. Privzemimo oznake kot zgoraj. Želeli bi dokazati, da je $(x^e)^d \equiv x \mod n$. Z upoštevanjem pravil za potenciranje in zgornjih zvez dobimo:

$$(x^e)^d = x^{de} = x^{km+1} = x^{km}x = x^{km}x.$$

Ločimo dva primera.
Če p ne deli x, tedaj po izreku 1 sledi, da je

$$x^m = (x^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \mod p$$

$$\Rightarrow x^{km+1} \equiv x \mod p$$

kar smo želeli dokazati.

Če p ni tuj proti x, tedaj mora deliti x in vse njegove potence:

$$p|x^{km+1},$$

iz česar sledi:

$$p|x^{km+1} - x.$$

Po definiciji kongruenc je to ravno

$$x^{km+1} \equiv x \mod p.$$

Enako preverimo še za q in dobimo

$$x^{km+1} \equiv x \mod q,$$

kar je ekvivalentno

$$q|x^{km+1} - x.$$

Ker sta p in q različni praštevili, iz pravil o deljenju sledi $n = pq|x^{km+1} - x$ oz.

$$x^{km+1} \equiv x \mod n.$$

□

3 Zaključek

S pomočjo sodobnih metod kodiranja so sporočila bolj ali manj varna pred vsiljivci ("hekerji"). Metode se sicer ves čas izboljšujejo, a zločinci so tudi tu ves čas korak pred zaščitniki. V prihodnosti bo programska oprema zagotovo še napredovala in tu bo prišla na vrsto matematika, da predlaga nove, težko rešljive probleme. Del odgovornosti za našo varno prihodnost torej leži na plečih matematikov.

Literatura

[1] J. A. Buchmann: *Introduction to cryptography*, Springer-Verlag NY, 2004.