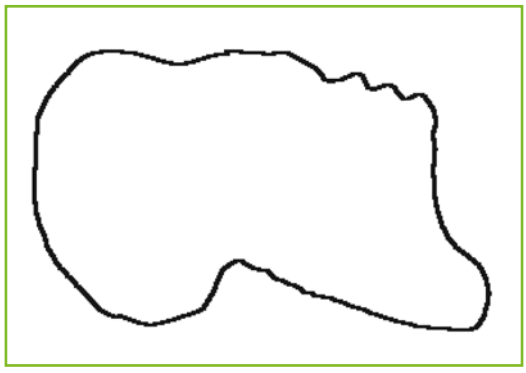
Vizualna kriptografija - Šum skrivnosti

MARTIN PEČAR

→ Predstavljajte si, da izhajate iz rodbine kapitanov Sinjebradcev, ki so jim legende pripisovale bajna bogastva. To bogastvo pa žal vas ni doseglo, saj je eden od Sinjebradcev, kot zgleden gusarski kapitan, zaklad namesto v sef švicarske banke zakopal v nedrja zemlje enega od otokov. Na srečo pa na podstrešju najdete del zemljevida...

Najprej si oglejmo, s čim se sploh ukvarja kriptografija. Pošiljatelj (Sinjebradec) ima sporočilo, polno skrivnih informacij, zato ga po šifrirnem sistemu zašifrira (raztrga zemljevid) in dobi tajnopis. Ta tajnopis pošlje naslovniku (svojim potomcem), ki ga odšifrira (zloži kose zemljevida) in prebere sporočilo. Ves čas pa na tajnopis prežijo tudi napadalci, ki bi se radi dokopali do skrivnih informacij ali pa naslovniku podtaknili lažne informacije. Kriptografi pa so tisti, ki tekmujejo v sestavljanju in izboljševanju šifrirnih sistemov ter iskanju napadov na te sisteme.

Vsi šifrirni sistemi, ki se zanašajo na *računsko varnost*, temeljijo na tem, da po določenem sistemu „premešajo“ informacijo oz. sporočilo. Ključ imenujemo podatke (parametre), ki v okviru danega šifrirnega sistema (algoritma) natančno določajo, kako iz sporočila narediti tajnopis in kako potem vrniti premešano informacijo oz. tajnopis v prvotno obliko. Ključ je običajno precej krajši od sporočila, sistem pa je tem boljši, čim več možnih ključev mora napadalec preizkusiti na poti do rešitve. Ob tem je smiselno upoštevati *Kerckhoffov princip*, ki predpostavlja, da napadalec pozna uporabljeni šifrirni sistem, ne pa tudi ključa. Napadalec ve, kdaj je prišel na cilj: ko ima tajnopis, razvozlan po določenem sistemu,



SLIKA 1.
Zemljevid otoka

SLIKA 2.
Križec označuje skriti zaklad

smiseln pomen, je to zelo verjetno izvorno sporočilo. Verjetnost, da bi dobil smiselno, a napačno sporočilo, je neznatna, če je le tajnopis dovolj dolg. Mogoče je pokazati, da je pri sistemu, kjer vsako črko nadomestimo z neko drugo črko oz. zamenjamo abecedo, za angleško sporočilo potrebna dolžina približno 25 črk.

Vrnimo se k zakopanemu zakladu. Če je najdeni del zemljevida dovolj velik, boste lahko prepoznali otok. Na najdenem delu pa žal ni označenega mesta, kje točno je zaklad zakopan. Gotovo bi vam skrito bogastvo prišlo zelo prav, zato lahko vzamete kramp in lopato, se odpravite na otok ter ga vsega prekopljete. Kriptografi bi to imenovali napad z grobo silo, saj morate v okviru informacije, ki jo imate (uporabljeni šifrirni sistem oz. ime otoka), preizkusiti vse možnosti (uporabiti vse mogoče ključe oz. prekopati vsak kvadratni meter). Če boste problemu namenili dovolj najlepših let svojega življenja, boste zaklad prej ali slej našli.

Vsi, ki želite zakopati zaklad na skrivnem mestu, pa lahko iskalcem še bolj otežite delo, če boste le prebrali nadaljevanje članka. Seveda pa ga lahko preberete tudi le iz radovednosti.

Ker nismo gusarji stare šole, bomo zemljevide namesto na pergament risali na prosojnice. Neuki Sinjebradec bi zemljevid na prosojnici verjetno narisal takole: na eno prosojnico sliko otoka, na drugo pa križec, ki označuje zakopani zaklad (slika 1, slika 2).

Ko prosojnici poravnamo in prekrijemo, je skrivnost razkrita. Tudi vsaka prosojnica zase razkrije nekaj informacije. Tako nam prva razkrije, na katerem otoku nas čaka zaklad. V nadaljevanju se bomo naučili, kako prosojnici porisati tako, da z vsake posebej nihče ne bo mogel pridobiti nikakršne informacije, obe skupaj pa bosta razkrili skrivnost (takorekoč 0 + 0 = 1).

V prejšnjem stoletju so se kriptografi domislili, kako informacijo zakriti tako, da je brez ključa nihče ne bo mogel razkriti. V kriptografiji temu pravimo *popolna varnost*. Dosežemo jo tako, da informacijo "zlijemo" s povsem naključnimi podatki. Tako onemogočimo napadalce, saj morajo le-ti odstraniti naključne podatke, s čimer pa lahko dobijo povsem drugačno sporočilo (primer 1). Ob danem tajnopisu je vsako sporočilo iste dolžine enako verjetno. V tajnopisu lahko najdeš, karkoli iščeš, zato ni več samo ene smiselne rešitve. Tajnopis pa odšifriramo tako, da odstranimo prej dodane naključne podatke.

Primer 1. Pravi ključ je ključnega pomena, četudi je naključen.

k r u h = *P* (1. sporočilo)	v i n o = *P'* (2. sporočilo)
a s k f = *K* (1. ključ)	n b s ž = *K'* = K + P - P (2. ključ)
l k h o = *C* (tajnopis)	l k h o = *C* (tajnopis)

V primeru 1 se zlivanje istoležnih črk (navpično)

izvede kot seštevanje zaporednih številk črk v abecedi ('k' + 'a' = 'l', saj je 12 + 1 = 13), kjer se ta ciklično ponavlja (za 'ž' pride spet 'a'). Če napadalec prestreže tajnopis C, ne more določiti sporočila, ker sta oba ključa K in K' (s tem pa tudi sporočili P in P') enako verjetna, saj sta naključna. Kdor pa pozna ključ, lahko odkrije sporočilo tako, da od tajnopisa odšteje ključ.

Največji problem pri tem šifrirnem sistemu je dolžina ključa — ključ je enako dolg kot sporočilo samo. Pri drugih sistemih je ključ običajno bistveno krajši. Pri enoabecedni zamenjavi je potrebno npr. poznati le zamenjavo za vsako črko, pa lahko s temi manj kot 30-imi podatki zašifriramo in odšifriramo celotno knjigo.

Opisana shema za dosego popolne varnosti se imenuje enkratni ščit (angl. one-time-pad), saj ključ kakor ščit prekrije podatke, uporabimo pa ga lahko samo enkrat (tudi vitezi so morali polomljene ščite zamenjati). Če bi ga uporabljali večkrat, bi napadalec lahko podtaknil njemu poznano sporočilo P, potem pa iz prestreženega tajnopisa C izračunal ključ $K = C - P$. Če je ključ razkrit, sistem ne ponuja nobene varnosti več.

Vemo, da vsako sporočilo lahko zapišemo v dvojiškem zapisu, torej kot zaporedje ničel in enic. Prekrivanje z enkratnim ščitom se v dvojiškem zapisu na istoležnih bitih izvede kot dvojiški *izključni (ekskluzivni) ali XOR* (tabela 1).

XOR	0	1
0	0	1
1	1	0

TABELA 1.
Izključni ali

OR	0	1
0	0	1
1	1	1

TABELA 2.
Ali

Izvorno sporočilo razkrijemo tako, da tajnopis še enkrat prekrijemo s ključem, saj je pri dvojiškem zapisu seštevanje enako odštevanju.

Leta 1994 sta se znana kriptografa Adi Shamir, soiznajditelj sistema javne kriptografije RSA, in Moni Naor domislila *vizualne kriptografije*. Ideja je podobna enkratnemu ščitu, le da namesto zaporedja bitov uporabimo ravnino, tlakovano s črnimi in belimi ploščicami, ki predstavljajo vrednosti bitov. Poleg tega pa namesto operacije 'izključni ali' (XOR) uporabimo operacijo navadni *ali OR* (tabela 2).

Na ta način slike zašifriramo, ko pa jih odšifriramo, so malce spremenjene, a še vedno prepoznavne. Najpomembneje pa je, da je vizualna kriptografija po sistemu enkratnega ščita podedovala *popolno varnost*. To pomeni, da napadalec ne more prepoznati zašifrirane slike, četudi ima še tako veliko časa in računske moči. Slaba stran popolne varnosti pa je, da je ključ prav tako dolg (obsežen) kot samo sporočilo; zaradi tega ni bistvene razlike med ključem in zašifriranim sporočilom (primerjaj sliko 3 in sliko 4).

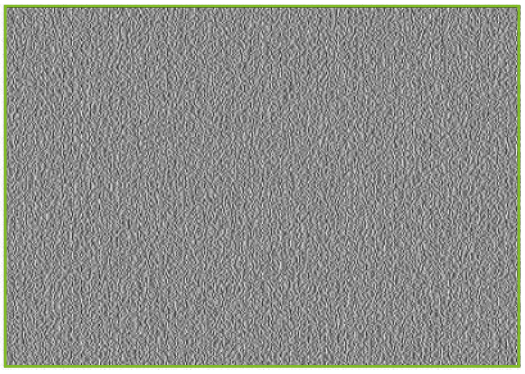
Poglejmo si idejo malce podrobneje: sliko bomo razstavili na dve različni, a enako veliki delni sliki (slika 3, slika 4). Vsako točko (angl. pixel) originalne slike bomo na obeh delnih slikah na istoležnih mestih nadomestili s ploščicama, ki imata eno polovico belo, drugo pa črno (tabela 3). Na prvi delni sliki bomo ploščico obrnili naključno, na drugi pa bo njena lega odvisna ob barve originalne točke in lege prve ploščice. Če je bila originalna točka bela, bo lega druge ploščice enaka legi prve, sicer pa jo položimo zrcalno. Z malo razmisleka ugotovimo, da sta legi obeh ploščic naključni, saj smo za prvo to privzeli, drugo pa smo položili glede na prvo, ki leži naključno.

Dešifriranje poteka nekoliko drugače. Predstavljajmo si, da mrežo ploščic narišemo na prosojnico, nato pa, če je ploščica (oz. njen del) črna, ustrezajoči del na prosojnici pobarvamo s črno barvo. Potem obe prosojnici prekrijemo. Kjer je bila vsaj ena od prosojnic pobarvana, vidimo črno, drugje pa je prosojno. Kjer se prekrijeta enako obrnjeni ploščici (npr. prva v zgornji vrstici in druga v spodnji vrstici sivo. Kjer pa se prekrijeta različno obrnjeni ploščici

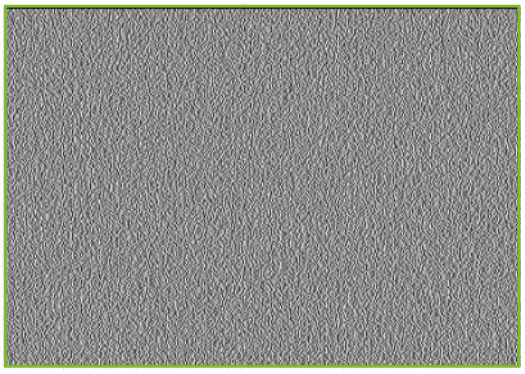
verjetnost	$p = 0.5$		$p = 0.5$	
na prvi delni sliki				
originalna slika	črno	belo	črno	belo
na drugi delni sliki				

TABELA 3.
Po shemi točko za točko postopno gradimo delni sliki

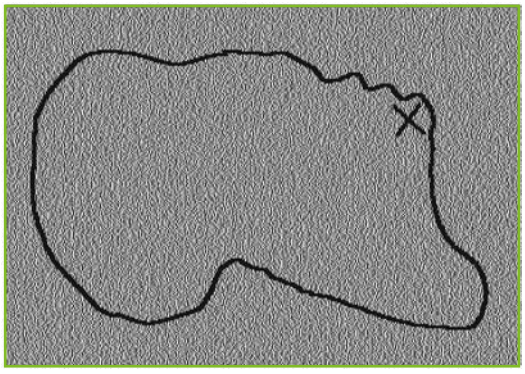
tabele 3), tam oko majhno črno-belo polje vidi kot



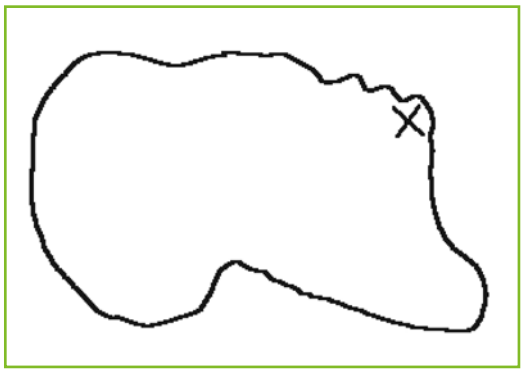
SLIKA 3.
Prva delna slika



SLIKA 4.
Druga delna slika



SLIKA 5.
Zlita slika oziroma prekriti delni sliki razkrijeta skrivnost



SLIKA 6.
Originalna slika

(npr. prva v zgornji vrstici in prva v spodnji vrstici tabele 3), pa vidimo črno polje.

Torej: originalno sliko razbijemo na dve enako veliki delni sliki, na katerih je vsaka točka naključno bela ali črna (to imenujemo šum). Ko obe delni sliki prekrijemo, zagledamo skrito podobo. Ta podoba je malce spremenjena (slika 5), saj tam, kjer so bile na originalni sliki bele ploščice, dobimo napol črne. Če so ploščice dovolj majhne, oko napol črne ploščice vidi kot sive. Torej iz črno-bele slike dobimo črno-sivo sliko. Kljub tej izgubi kontrasta so enostavne slike še vedno prepoznavne.

Opisali smo osnovno idejo vizualne kriptografije. Kmalu pa so se začele pojavljati nadgradnje te zamisli. Prvo sta podala že Naor in Shamir v svojem članku. Kako zašifrirati sliko, ki ni le črno-bela, ampak vsebuje tudi sive tone? Možen odgovor je: uporabimo okrogle ploščice. Na prvi delni sliki ploščico zavrtimo za naključen kot. Na drugi delni sliki jo položimo enako, če je originalna ploščica bela (prekriti prosojnici bi pokazali napol črn krog), nasprotno, če je originalna ploščica črna (prekriti prosojnici pokažeta črn krog), in ustrezno zavrteno (prosojnici pokažeta krog, katerega več kot polovica je črna) ob ustrezno sivi ploščici (tabela 4). Na ta način dobimo novo prostostno stopnjo (zvezne tone sivine) z (zveznim) vrtenjem ploščic. Žal pa je ta način, čeprav zelo eleganten, precej neprikladen za izvedbo s pomočjo računalnika, zato so nove ideje zelo dobrodošle.

prvi del	drugi del	prekrito
		

TABELA 4.
Okrogle ploščice nam omogočijo šifriranje sive slike

Deljenje skrivnosti

Vizualna kriptografija je tesno povezana s področjem deljenja skrivnosti (glej članek [1]). Spomnimo se zopet kapitana Sinjebradca; imel je tri sinove in namesto rentnega varčevanja jim je namenil del naropanega bogastva, ki ga je po stari gusarski šegi zakopal. Bal pa se je pretiranega pohlepa sinov. Ker je želel ohraniti vsaj nekaj družinske sloge, naj bi pri izkopavanju zaklada sodelovala vsaj dva brata; en sam se ne bi mogel polastiti vsega bogastva. Zato je (proti koncu članka že bolj kriptografsko vešč) ka-

pitan zemljevid razdelil na tri delne slike na prosojnicah tako, da se skrivnost razkrije, ko sta prekriti vsaj dve delni sliki. To je t. i. *shema 2-od-3*. Možno je skonstruirati tudi bolj zapletene sheme, ki so sestavljene iz več delnih slik, med katerimi so lahko nekatere bolj, druge pa manj pomembne. Oglejmo si preprost primer konstrukcije sheme 2-od-3 (tabela 5, tabela 6).

Ko gradimo tri delne slike, za vsako točko uporabimo tabelo 5, če je točka na originalni sliki črna (ima vrednost 1), oz. tabelo 6, če je točka bela (ima vrednost 0); stolpce izbrane tabele naključno premešamo, vrstice premešane tabele pa zaporedoma predstavljajo ploščice na posameznih delnih slikah (slika 7). Enostavno povedano: če je originalna točka bela, so na delnih slikah istoležni kosi ploščic enaki,

1	0	0
0	1	0
0	0	1

TABELA 5. Šifriranje črne točke.

1	0	0
1	0	0
1	0	0

TABELA 6. Šifriranje bele točke.

SLIKA 7. Ploščica, ki prestavlja drugo vrstico tabele 5(010).

če pa je bila črna, se istoležni kosi razlikujejo. V vsakem primeru pa so naključno razporejeni. Tu gre po eni strani za varnost (vsaka ploščica na delni sliki je 1/3 črna), po drugi pa za kontrast. Če prekrijemo ploščici na delnih slikah, ki predstavljata originalno belo točko, namreč dobimo 1/3 črno ploščico, če pa predstavljata originalno črno točko, dobimo 2/3 črno ploščico – kontrast je 1/3. Podrobnejše napotke je moč najti v članku [2]. Članki o barvni vizualni kriptografiji in drugih zanimivostih pa so dosegljivi tudi na spletu z iskanjem po ključnih besedah *visual cryptography* in *secret sharing*. Če bi kapitan Sinjebradec redno bral Presek, bi gotovo vedel, kako doseči popolno varnost za svoje skrivnosti. Morda pa bi ga branje tako prevzelo, da bi mu zmanjkalo časa za gusarske podvige.

Literatura

[1] A. Jurišić, *Kako deliti skrivnosti*, Presek **29** 2002, 6, 358–364.

[2] D. Stinson, *Visual cryptography & threshold schemes*, Dr. Dobb's Journal, april 1998, 36–43.

×××

×××

→ → →

SLIKE K ČLANKU PREGLED PRISPEVKOV