Kriptografija i teorija brojeva

Žarko Mijajlović
zarko.mijajlovic@gmail.com

Kolarčev univerzitet
proleće 2016

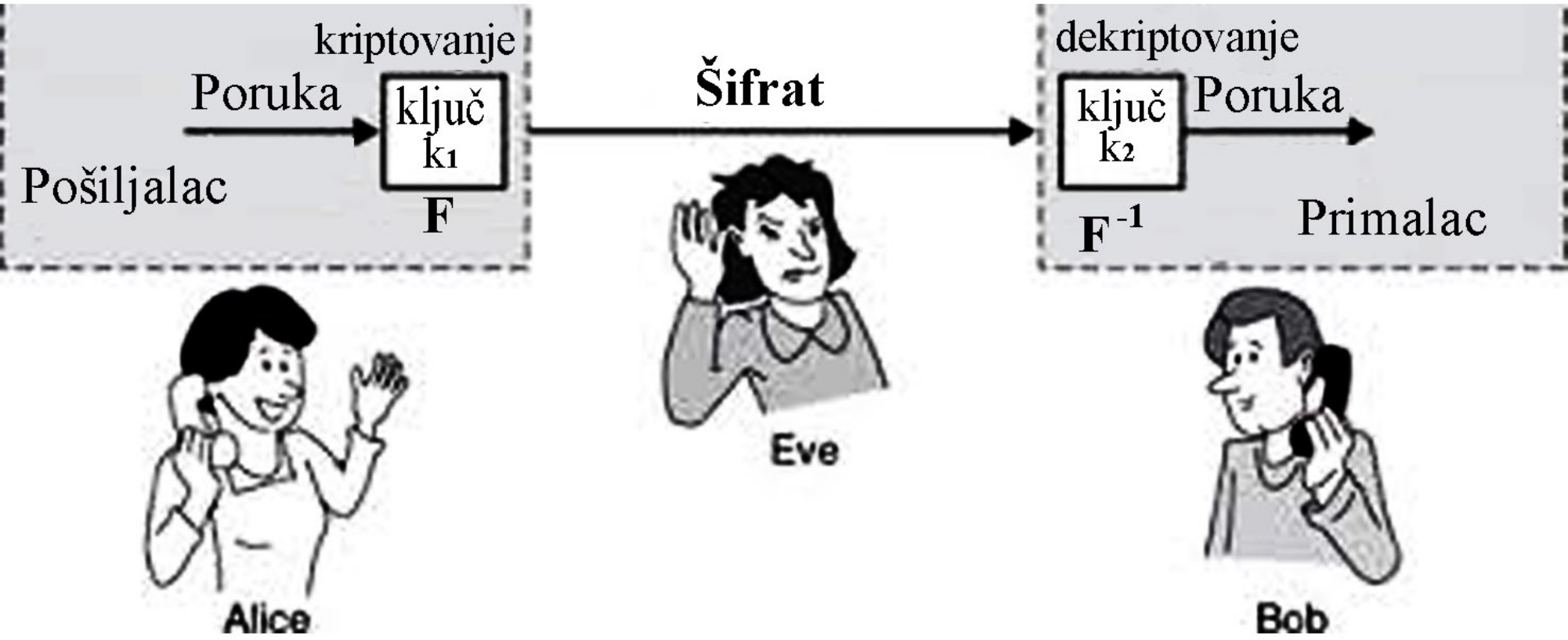
Kriptografija: definicija

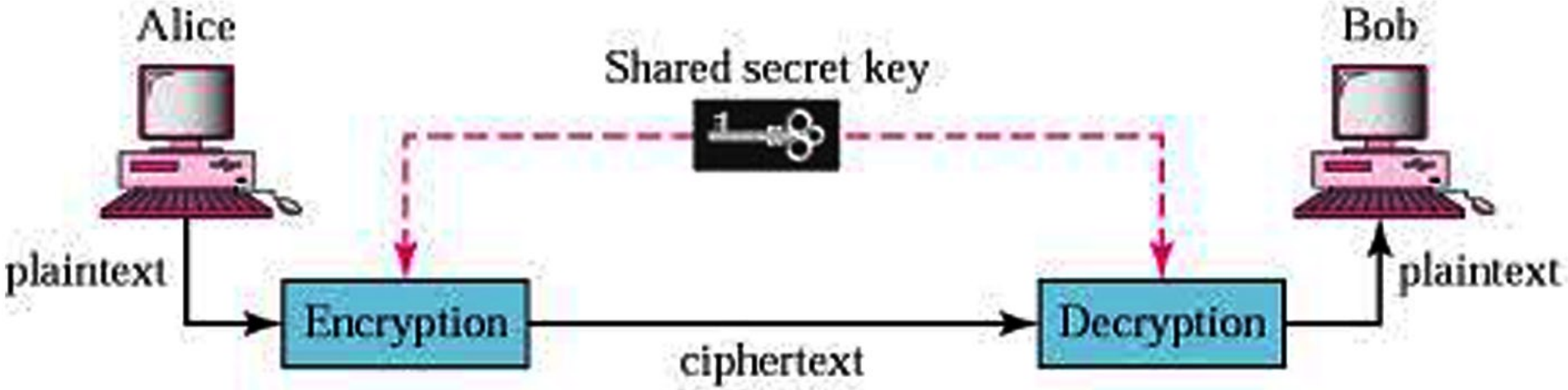
Kriptografija je veština i nauka da se određena informacija – poruka prosledi na tajan način. Pod ovim podrazumevamo sledeći scenario.

Pošiljalac **A** (Alisa) treba da dostavi određenu poruku P primaocu **B** (Bob) ali tako da neprijatelj **I** (Iva, od "Eavesdropping" - prisluškivanje) koji ima pristup toj komunikaciji praktično nema mogućnosti da sazna sadržaj poruke P.

U tu svrhu Alisa nekim postupkom (algoritmom, funkcijom, protokolom) F koristeći ključ k_1 **kriptuje** (prevodi, transformiše) originalnu poruku P u šifrat - kôd S i Bobu zapravo prosleđuje tekst S.

Bob primenjuje inverzan postupak F^{-1} uz pomoć ključa k_2 na S i tako **dekriptuje** – nalazi originalan tekst P.


kriptovanje
Poruka
ključ
k1
F
Pošiljalac
Šifrat
dekriptovanje
ključ
k2
Poruka
F -1
Primalac
Eve
Alice
Bob


Alice
Shared secret key
Bob
plaintext
Encryption
ciphertext
Decryption
plaintext

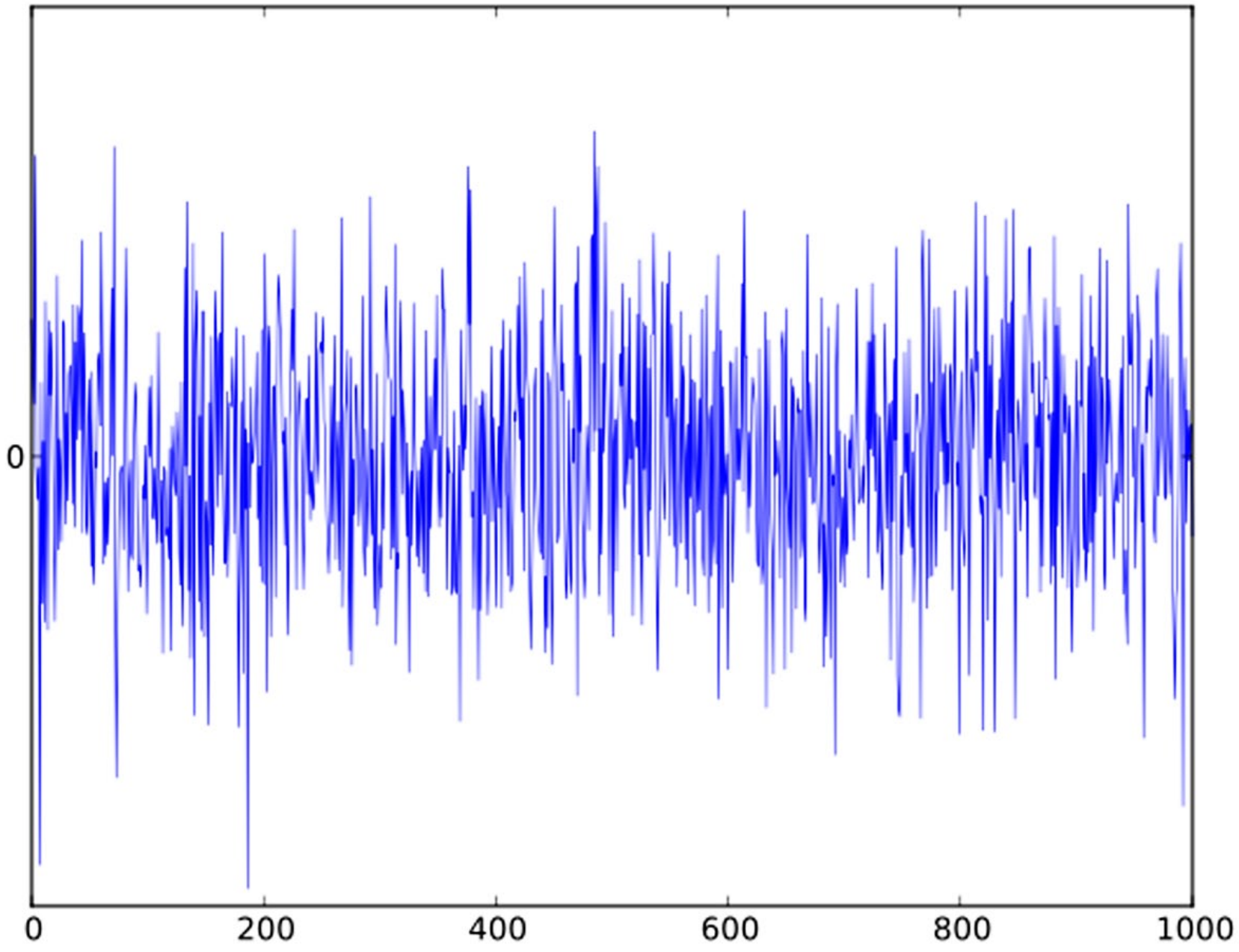
Kriptografija: definicija

Iva u komunikaciji između Alise i Boba ima pristup samo šifratu S. Kriptovanje treba da bude tako dizajnirano, da Iva, pa i da zna kriptujuću funkciju funkciju F, **bez poznavanja ključa k_2 nije u mogućnosti da razbije šifru** S tj. sazna originalnu poruku P.

Dobri kriptografski sistemi podrazumevaju:

- Kriptovana poruka treba da što je moguće više liči na šum - slučajan signal sa uniformnom verovatnosnom distribucijom.
- Funkcija F^{-1} treba da bude tako računski složena da bez poznavanja ključa k_2 nije moguće njeno izračunavanje u realnom vremenu.

Tradicionalni kriptografski sitemi podrazumevaju da su ključevi k_1 i k_2 isti i tajni. Otuda se ovi sistemi nazivaju simetričnim i poznati su kao kriptografski sistemi sa tajnim ključem.


0
0
200
400
600
800
1000

Kriptografija sa tajnim ključem

Principi:

- Funkcija (postupak, algoritam) F kojom se ostvaruje kriptovanje je tajna.
- Ključ (lozinka) je tajna.
- Pomoću istog ključa vrši se kriptovanje i dekriptovanje.
- Oba ova entiteta, funkcija i ključ, treba da budu poznati samo pošiljaocu i primaocu poruke.

S obzirom da se koristi isti ključ za kriptovanje i dekriptovanje, ovakvi sistemi nazivaju se takođe **simetričnim kriptografskim sistemima**.
Problem: Kako dostaviti ključ primaocu poruke?

Kriptografija sa privatnim ključem

Primer (šifra Julija Cezara)

Funkcija F_k: Ciklična permutacija alfabeta za k mesta

$$F_3 = \begin{pmatrix} A & B & C & D & \dots & V & W & X & Y & Z \\ D & E & F & G & \dots & Y & Z & A & B & C \end{pmatrix}$$

Ovde za ključ možemo uzeti $k = 3$.

Tada $F_3 : \mathrm{IBM} \to \mathrm{LEP}$, $F_3^{-1} : \mathrm{LEP} \to \mathrm{IBM}$.

Slično za $k = -1$ (Odiseja 2001):

$$F_{-1} = \begin{pmatrix} A & B & C & D & \dots & V & W & X & Y & Z \\ Z & A & B & C & \dots & U & V & W & X & Y \end{pmatrix}$$

$F_1 : \mathrm{IBM} \to \mathrm{HAL}$.

Kriptovanje sa privatnim ključem

Sve do **osamdesetih godina prošlog veka** koristili su se isključivo sistemi s tajnim ključem.

Šifarski sistem opisan u prethodnom primeru **lako se razbija**, pa i da se uzme proizvoljna permutacija alfabeta. Na primer, **statističkom analizom** frekvencija pojaljivanja simbola u šifratu.

Ipak, u većini simetričnih kriptografskih postupaka koriste se kombinatorne sheme zasnovane na permutacijama. Važno mesto u ovim postupcima, naročito u generisanju ključeva imaju **pseudoslučajni brojevi**.

Čuveni primer uređaja koji se koristio u kriptografiji sa privatnim ključem je **elektromehanička mašina Enigma** koju je patentirao nemački inženjer Arthur Schrebius 1918. Razne verzije ove mašine koristile su se u Nemačkoj u komercijalne i vojne svrhe, sve do završetka Drugog svetskog rata.

Enigma


Crypto Museum
cryptomuseum.com

Kriptovanje sa javnim ključem

Principi:

- Postoje dva različita ključa, jedan za kriptovanje, drugi za dekriptovanje.
- Ključ za kriptovanje je javno dostupan.
- Ključ za dekriptovanje čuva se u tajnosti i dostupan je samo entitetu koji vrši dekriptovanje.
- Generisanje ključeva treba da bude relativno jednostavno.
- Kriptovanje i dekriptovanje treba da budu računski jednostavne operacije.
- Razbijanje koda (šifrata) treba da bude računski veoma teško izvodljivo u realnom vremenu.

Kriptovanje sa javnim ključem

Kriptografski sistemi sa *javnim ključem* poznati su takođe pod nazivom **asimetrični kriptografski sistemi**.

Osnovna odlika ovih sistema je da entitet[1] **B** (Bob) koji prima poruku poseduje **javni-kriptujući ključ** e i odgovarajući - korespodentni **privatni-dekriptujući ključ** d.

Glavna ideja sigurnosti sistema ove vrste je da izračunavanje - određivanje privatnog ključa d za poznat javni ključ e **predstavlja neizvodljiv zadatak**, s obzirom na raspoložive tehničke resurse, vreme i poznate matematičke metode. Ovo svojstvo je glavna razlika u odnosu na simetrične sisteme, pa otuda i naziv asimetrični sistemi.

[1] korisnik, kompjuter, ustanova.

Kriptovanje sa javnim ključem

Javni ključ e određuje transformaciju kriptovanja E_e, dok s druge strane privatni ključ d definiše njoj pridruženu, dekriptujuću transformaciju D_d. Preslikavanje D_d je inverzna funkcija za E_e, tj. ako je $f = E_e$ onda $f^{-1} = D_d$.

Entitet **A** (Alisa) koji ovim sistemom šalje poruku (osnovni tekst) m entitetu **B** (Bobu), mora imati na raspolaganju autentičnu kopiju javnog ključa e entiteta B.

Koristeći kriptujuću transformaciju E_e, **Alisa** proizvodi šifrat – kriptovanu poruku $c = E_e(m)$ koju zatim prosleđuje **Bobu**.

Po primanju poruke c, **Bob** primenjuje dekriptujuću transformaciju D_d i na taj način određuje originalnu poruku $m = D_d(c)$.

Vidimo da je jedan ovakav sistem, koji je u potpunosti određen svojim ključevima d i e, pogodan za jednosmernu komunikaciju, tj. za slanje kriptovanih poruka u jednom pravcu, od **A** prema **B**.

Kriptovanje sa javnim ključem

U antisimetričnim sistemima, javni ključ e nije tajan, zapravo može biti široko rasprostranjen, i u procesu kriptovanja ne zahteva se sigurnost i tajnost u transferu javnog ključa. Zato se ovi sistemi nazivaju i sistemima sa otvorenim ključem.

Ovim se izbegavaju uobičajene teškoće u koje se javljaju u sigurnom prenosu ključeva koje se pojavljuju kod drugih sistema. Zahteva se samo **autentičnost javnog ključa** e, čime se garantuje da je **Bob** jedini u posedu korespodentnog-privantog ključa d.

To znači da u okviru jednog ovakvog sistema kriptovanja, **Bob** mora biti siguran da je dobijena kriptovana poruka c zaista poslata od strane njegovog partnera – **Alise**, a ne od nelegalnog entiteta, *neprijatelja* **Ive**.

Kriptovanje sa javnim ključem

Glavna prednost ovakvih sistema u odnosu na simetrične i uopšte tradicionalne sisteme je, u osnovi jednostavan način obezbeđivanje javnog ključa (doturanje ključa e strani **Alisi**).

Taj ključ se može objaviti bilo gde, na primer u telefonskom imeniku, ili što je praktičnije, u listama sa poštanskim adresama ili kompjuterizovanim sistemima prenosa poruka (e-mail, internet adrese, bankovni automati, ...).

S druge strane, u toj činjenici krije se i **glavna slabost ovakvih sistema**. Naime, s obzirom da je javno poznata kriptujuća transformacija entiteta B, javni-kriptujući ključ ne obezbeđuje autentičnost originalne poruke, odnosno integritet te poruke. Otuda se autentičnost poruka mora obezbediti drugim sredstvima, kao što su poruka o autentičnosti kôda i digitalni potpis.

Kriptovanje sa javnim ključem

Kriptografski sistemi sa javnim ključem **po pravilu su mnogo sporiji** od algoritama simetričnih sistema, kao što je sistem DES, na primer.

Iz tog razloga, sistemi sa javnim ključem **koriste se u ograničenim i specifičnim situacijama**, kao što je dotur ključeva za sisteme koji se koriste za kriptovanje masivnih podataka. Ili kriptovanje malog broja podataka – kratkih poruka, kao što je brojevi kreditnih i bankovnih kartica.

Isto tako, sistemi sa javnim ključem mogu se koristiti za obezbeđivanje identifikacije u procesu autentifikacije entiteta, a takođe kao autentifikacioni ključ u protokolima uspostavljanja komunikacije.

Kriptografija i teorija informacija

U svom čuvenom radu *A mathematical theory of communication* (1948) Claude Shannon, osnivač matematičke teorije informacije, diskutovao je sigurnost šifarskih sistema.

Shannon je tamo pokazao da uz izbor odgovarajućih ključeva, mada se kriptovana poruka u principu (teorijski) može razbiti, ona je ipak sa praktične strane sigurna, s obzirom da je broj matematičkih operacija potreban za probijanje ključa ekscesno veliki.

Kodirane poruke kriptovane sistemima sa otvorenim ključem predstavljaju ekstreman slučaj u odnosu na vezu između veličine ključa i računske složenosti za **lvu** dekriptora.

Naime, ne postoji nikakva ključna tajna informacija koju treba detektovati, već samo ogroman računski problem! U tom smislu, asimetrični sistemi mogu se smatrati kao kriptografski sistemi koji imaju (javne) ključeve čiji je informacioni sadržaj jednak nuli.

Kriptografija i teorija složenosti

Uloga složenosti izračunavanja u asimetričnim sistemima ukazuje na važnost i primenljivost u ovoj oblasti, rezultata tzv. **teorije složenosti**, grane teorije formalne izračunljivosti.

Primer takve vrste jeste poznati problem $P = NP$, ili dokaz da je neki određen algoritam S **teško rešiv** ili **NP kompletan**. Drugim rečima da vreme njegovog rešavanja eskponencijalno raste u odnosu na veličinu ulaznih podataka.

Bilo koji dokaz (u matematičkom smislu) da se postupci za razbijanje kriptovanog teksta svode na teško rešiv S, ukazuje da je sa sigurnosne strane izabrani algoritam kriptovanja korektan.

Ipak, činjenica je da je malo sistema sa javnim ključem za koje se znaju dokazi ove vrste. Tako možemo razumeti određene rezerve kod pojedinih eksperata u ovoj oblasti, koji ukazuju da je moguće da se jednom otkrije neki postupak pogodan za probijanje kriptovanog kôda datog sistema sa javnim ključem.

Primena teorije brojeva u kriptologiji

Već u simetričnim kriptološkim sistemima značajno mesto ima **teorija brojeva**, na primer u razvoju algoritama za generisanje pseudoslučajnih brojeva koji su neophodni na primer za generisanje ključeva.

Kod asimetričnih sistema teorija brojeva ima glavno mesto ne samo u generisanju ključeva već i za dizajn samog kriptološkog algoritma, ali i u kriptološkoj analizi.

Ključno mesto ima **modularna aritmetika**, tj. prsten ostataka po modulu n, $n \geqslant 2$, $\mathbf{Z}_n = (Z_n, +_n, \cdot_n, 0, 1)$, $Z_n = \{0, 1, 2, \ldots, n-1\}$.

$x +_n y = \mathrm{rest}(x + y, n), \quad x \cdot_n y = \mathrm{rest}(x \cdot y, n).$
$\mathrm{rest}(a, n) =$ celobrojni ostatak dobijen deljenjem broja a brojem n.
Definicija: $a = b \,(\mathrm{mod}\, n)$ akko $\mathrm{rest}(a, n) = \mathrm{rest}(b, n)$.

Primer: $\mathrm{rest}(11, 7) = 4, \quad 4 +_7 6 = 3, \quad 5 \cdot_7 6 = 2.$

Primena teorije brojeva u kriptologiji

Mala Fermaova teorema (Pierre Fermat, 1601-1665)
Neka je p prost broj i $n \geqslant 1$ prirodan broj, uzajamno prost sa n. Tada $n^{p-1} = 1 \pmod{p}$.

Druga formulacija: Ako je p prost broj, tada je $\mathbf{Z}_p$ polje i u tom polju važi: ako je $x \neq 0$, tada je $x^{p-1} = 1$.

Ojlerova funkcija $\varphi(n)$. (Leonhard Euler, 1707-1783) Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ razlaganje prirodnog broja n na proste faktore, tada

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Primer. $8^4 = 1 \pmod{5}$, $\quad n = 847 = 7 \cdot 11^2$,
$\varphi(n) = 11 \cdot (7 - 1) \cdot (11 - 1) = 660$.

Pierre Fermat

Leonhard Euler

Primena teorije brojeva u kriptologiji

Carl Fridrich Gauss (1755-1855) uveo je račun kongruencija - modularnu aritmetiku.

Modularna aritmetika zajedno sa nekoliko osnovnih teorema i postupaka kao što su Euklidov algoritam, Ojelrova funkcija i Mala Fermaova teorema omogućava da se predstave glavne ideje savremene kriptografije.

Slučajni brojevi i nizovi imaju veliku ulogu u kriptologiji. Oni ne nose nikakvu informaciju i zato su pogodni za skrivanje originalne, nama važne poruke. Dosta je teško proizvesti prave slučajne nizove i u tu svrhu koriste se uređaji koji mere prirodne pojave slučajne prirode, na primer kosmičko zračenje i radioaktivnost.

Koristeći modularnu aritmetiku moguće je algoritamski proizvesti nizove koji naravno nisu slučajni ali prolaze statističke testove slučajnosti pa se mogu koristiti umesto slučajnih nizova. To su **pseudo-slučajni nizovi**.

Primena teorije brojeva u kriptologiji

Na primer, za dobro izabrane a, c, m i početnu vrednost X_0, **linearnom diferencijskom kongruencijskom jednačinom**

$$X_{n+1} = (aX_n + c) \pmod m$$

možemo generisati pseudo-slučajni niz.

Primer. $X_{n+1} = (22695477 \cdot X_n + 1) \pmod{2^{32}}$, X_0 proizvoljno.

Zgodno je da se ovom formulom generiše što duži niz, koji, jasno, ne može imati dužinu veću od m. Imaće baš dužinu m akko:

- a i c su uzajamno prosti.
- Svaki prost faktor broja m je i prost faktor broja $a - 1$.
- Ako 4 deli m, tada 4 deli $a - 1$.

Primer jednog simetričnog kriptološkog sistema

U opštem slučaju, zbir dva niza od kojih je jedan slučajan proizvodi slučajan niz. To važi i ako su članovi niza bitovi 0, 1, a primenjujemo aritmetiku po modulu 2:

Poruka: $\mathbf{a} = a_0, a_1, a_2, \ldots, a_n$

(Pseudo-)slučajan niz (šum): $\mathbf{s} = s_0, s_1, s_2, \ldots, s_n$

Zbir $\mathbf{b} = \mathbf{a} +_2 \mathbf{s} = a_0 +_2 s_0, a_1 +_2 s_1, a_2 +_2 s_2, \ldots, a_n +_2 s_n$ može se smatrati slučajnim nizom. Ako Alisa kroz etar šalje Bobu šifrat $\mathbf{b}$, tada se $\mathbf{b}$ utapa u radijacijsku okolinu i za potencijalnog napadača lvu $\mathbf{b}$ se ne razlikuje od šuma i ne nosi bilo kakvu informaciju.

Bob lako dešifruje $\mathbf{b}$ jer

$$\mathbf{b} +_2 \mathbf{s} = (\mathbf{a} +_2 \mathbf{s}) +_2 \mathbf{s} = \mathbf{a} +_2 (\mathbf{s} +_2 \mathbf{s}) = \mathbf{a} +_2 \mathbf{0} = \mathbf{a}.$$

Primer jednog simetričnog kriptološkog sistema

Primer Pretpostavimo da je poruka koju Alisa želi da pošalje Bobu $P =$ "RSA". ASCII kôd od P je 82 83 65, ili u binarnom zapisu

01010010 01010011 01000001

Dakle možemo uzeti da je $\mathbf{a} = 010100100101001101000001$.

Pretpostavimo da je Alisa koristeći pomenutu linearnu kongruenciju generisala uz početnu vrednost - ključ X_0 pseudo-slučajan niz $\mathbf{s} = 001100111101111100110110$.

Tada je šifrat $\mathbf{b} = \mathbf{a} +_2 \mathbf{s} = 011000011000110001110111$.

Alisa šalje Bobu šifrat $\mathbf{b}$ i odvojenim kanalom ključ X_0. Bob iz iste linearne kongruencije generiše isti pseudo-slučajan niz $\mathbf{s}$ i nalazi binarni kôd $\mathbf{a} = \mathbf{b} +_2 \mathbf{s}$ originalne poruke P, a odatle i samo P.

Decimal - Binary - Octal - Hex – ASCII Conversion Chart

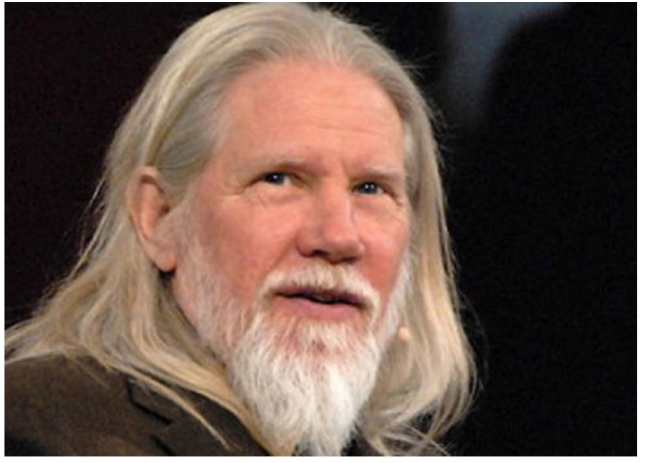
Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
0	00000000	000	00	NUL	32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
1	00000001	001	01	SOH	33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
2	00000010	002	02	STX	34	00100010	042	22	“	66	01000010	102	42	B	98	01100010	142	62	b
3	00000011	003	03	ETX	35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
4	00000100	004	04	EOT	36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
5	00000101	005	05	ENQ	37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
6	00000110	006	06	ACK	38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
7	00000111	007	07	BEL	39	00100111	047	27	‘	71	01000111	107	47	G	103	01100111	147	67	g
8	00001000	010	08	BS	40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
9	00001001	011	09	HT	41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
10	00001010	012	0A	LF	42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
11	00001011	013	0B	VT	43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
12	00001100	014	0C	FF	44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
13	00001101	015	0D	CR	45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
14	00001110	016	0E	SO	46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
15	00001111	017	0F	SI	47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
16	00010000	020	10	DLE	48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
17	00010001	021	11	DC1	49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
18	00010010	022	12	DC2	50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
19	00010011	023	13	DC3	51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
20	00010100	024	14	DC4	52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
21	00010101	025	15	NAK	53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
22	00010110	026	16	SYN	54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
23	00010111	027	17	ETB	55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
24	00011000	030	18	CAN	56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
25	00011001	031	19	EM	57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
26	00011010	032	1A	SUB	58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
27	00011011	033	1B	ESC	59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
28	00011100	034	1C	FS	60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
29	00011101	035	1D	GS	61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
30	00011110	036	1E	RS	62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
31	00011111	037	1F	US	63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Kriptografski sistemi sa javnim ključem

Pojam kriptografskog sistema sa javnim ključem uveli su **W. Diffie** i **M. Hellman** 1976 godine, i nezavisno **R. Merkle** 1978 godine. Do tog vremena ovi sistemi se nisu koristili niti su bili poznati. Od tada se pojavio relativno veliki broj kriptografskih sistema ove vrste.

Pojedini od ovih algoritama pogodni su samo za distribuciju ključeva, drugi se koriste za kriptovanje, dok su treći pogodni samo za digitalni potpis. Samo su dva algoritma pogodna i za kriptovanje i za digitalni potpis. To su sistemi **RSA** i **ElGamal**.

Navodimo kratak pregled nekoliko najpoznatijih kriptografskih sistema sa javnim ključem. Uz svaki od tih sistema dajemo osnovnu informaciju o matematičkoj osnovi, odnosno u čemu se sastoji računski problem za nelegalnog čitača kriptovane poruke.



Whitfield Diffie

Marty Hellman

Ralph Merkle

Kriptografski sistemi sa javnim ključem

RSA. Veza između osnovnog teksta i kriptovane poruke određena je strukturom prstena ostataka po modulu prirodnog broja n. Pouzdanost sitema sastoji se u težini problema faktorizacije velikih prirodnih brojeva na proste faktore.

Rabin. Algoritam je zasnovan na nalaženju kvadratnog korena datog prirodnog broja k u prstenu ostataka po modulu složenog prirodnog broja n. Ovaj zadatak ekvivalentan je problemu faktorizacije prirodnih brojeva pa se i ovde pouzdanost sitema sastoji u težini problema faktorizacije velikih prirodnih brojeva na proste faktore.

ElGamal. Ovaj algoritam je jedna modifikacija Rabinovog algoritma, samo umesto kvadratne funkcije u ovom slučaju uzeta je eksponencijalna funkcija. Pouzdanost sitema sastoji se u težini određivanja diskretnog logaritma za dati prirodni broj x u Galoaovom polju GF(p), gde je p prost broj.

Kriptografski sistemi sa javnim ključem

Generaliasani ElGamal. Algoritam je generalizacija ElGamalovog postupka. Naime, u ovom slučaju matematičku osnovu čine svojstva eksponencijalne funkcije u nekoj konačnoj cikličnoj grupi G. Pouzdanost sitema sastoji se u težini određivanja diskretnog logaritma u grupi G.

Kriptovanje pomoću eliptičkih krivih. Ovaj algoritam je specijalan slučaj generalisanog ElGamalovog algoritma u kojem grupu G čine tačke na eliptičkoj krivoj u konačnom polju. Pouzdanost sitema sastoji se u težini određivanja diskretnog logaritma u grupi G.

Merckle-Hellman knapsack (ranac). Algoritam je zasnovan na kombinatornoj teoriji brojeva i celobrojnim linearnim formama. Pouzdanost sitema sastoji se u težini rešenja tzv. problema podzbirova.

RSA: Rivest-Shamir-Adleman algoritam

RSA (Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman, 1977) je prvi praktično upotrebljiv asimetričan kriptografski sistem.

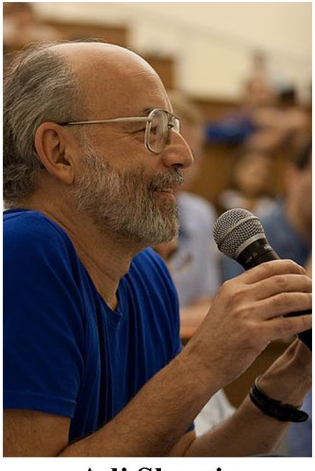
Ubrzo je ušao u široku upotrebu, pre svega za siguran prenos ključeva u simetričnim sistemima. **RSA je relativno spor, zato se koristi za kodiranje kratkih poruka**.

Rivest, Shamir i Adleman dobili su **Turingovu nagradu** za svoje otkriće.

Autori su patentirali svoj algoritam (!). Patent je istekao 2000. godine.

Engleski matematičar **Clifford Cocks** radeći za englesku obaveštajnu službu, otkrio je ekvivalentan algoritam 1973, ali je to otkriće objavljeno tek 1997. Dotle je Cocksov algoritam imao status vrhunske državne tajne.

Ronald Rivest



Adi Shamir

Leonard Adleman

RSA algoritam

Ideja RSA postupka: Bob, koji želi da primi poruku od Alice (ili bilo koga), bira dva velika prosta broja p i q (imaju po nekoliko stotina cifara) i pomoću njih nalazi javni ključ (n, e) i tajni ključ (n, d), gde je $n = pq$.

Ukoliko Alisa želi da Bobu pošalje poruku P na kriptovan način, najpre nalazi njen numerički kôd M, a zatim računa šifrat

$$C = M^e \pmod{n}$$

tj. računa stepen M^e u prstenu $\mathbf{Z}_n$.

Po prijemu šifrovane poruke C, Bob računa numerički kôd M

$$M = C^d \pmod{n}.$$

odakle nalazi originalnu poruku P.

RSA algoritam - otpornost na napad

Praktična upotrebljivost i otpornost RSA algoritma na napad počiva na sledećim činjenicama:

- Primalnost nekog prirodnog broja proverljiva je u polinomijalnom vremenu.
- Računski je veoma lako pomnožiti dva velika broja p i q, tj. izračunati $n = pq$.
- Za dobro izabrane i velike p i q računski je veoma teško da se uradi faktorizacija broja n, pa i da se zna da je n proizvod samo dva prosta broja.

Prosti brjevi p i q biraju se na slučajan način:

- Oba broja imaju bar po 150 cifara,
- Razlikuju se za par desetina dekadnih mesta. Na primer, p ima 150 cifara, dok q ima 170 cifara.

RSA: algoritam i matematičko obrazloženje

- Bob bira dva velika prosta broja p i q.
- Bob računa $n = pq$ i $m \equiv \varphi(n) = (p-1)(q-1)$.
- Koristeći Euklidov algoritam, Bob nalazi $e \in Z_m$ takav da je $\mathrm{NZD}(e, m) = 1$.
- Koristeći Euklidov algoritam, Bob nalazi $d \in Z_m$ tako da je $e \cdot_m d = 1$, tj. $ed = 1 \pmod{n}$. To je moguće jer su e i m uzajamno prosti.
- Bob objavljuje svoj javni ključ (n, e) i za sebe u tajnosti čuva tajni ključ (n, d).

Lema. Prema Maloj Fermaovoj teoremi za svaki prirodan broj $M < n$ važi $M^{ed} = M \pmod{n}$.

RSA: algoritam i matematičko obrazloženje

- Alisa za kratku poruku P koju želi da pošalje Bobu, nalazi njen numerički kôd $M < n$. Numerički kôd nalazi koristeći na primer ASCII tabelu. Ukoliko Alisa želi da pošalje dužu poruku, onda je deli na blokove tako da je numerički kôd svakog bloka manji od n.
- Alisa nalazi šifrat $C = M^e$ u prstenu $\mathbf{Z}_n$, tj. $C = M^e \pmod{n}$.
- Alisa šalje Bobu šifrat C bilo kako, pa i koristeći javnu komunikaciju.
- Po prijemu šifrata C, Bob računa M:

  $C^d = M^{ed} = M \pmod{n}$.

  Lema obezbeđuje tačan račun.
- Koristeći ASCII tabelu, Bob iz numeričkog kôda M nalazi originalnu poruku C.

RSA: Primer

- Bob bira proste brojeve $p = 59, q = 71$.
- Bob računa
  $n = 59 \cdot 71 = 4189, \quad m \equiv \varphi(n) = (59-1)(71-1) = 4060.$
- Bob bira broj $e = 671$ koji je uzajamno prost sa m.
- Bob u prstenu $\mathbf{Z}_m$ računa $d = e^{-1} = 1791$ koristeći Euklidov algoritam.
- Bob distribuira javni ključ $(n, e) = (4189, 671)$ i čuva u tajnosti svoj ključ $d = 1791$.
- Bobova kriptujuća funkcija je $E(M) \equiv M^{671} \pmod{4189}$, uz uslov $0 \leqslant M < 2^{12} - 1 = 4095$.
- Bobova dekriptujuća funkcija je $D(M) \equiv M^{1791} \pmod{4189}$, uz uslov $0 \leqslant M < 2^{12} - 1 = 4095$.

Napomena. Obe funkcije E i D izračunavaju se u najviše $2\log_2(n)$ primena modularnog množenja $\cdot_m$.

RSA: Primer

Alisa šifruje i šalje Bobu poruku RSA na sledeći način:

- RSA $= 82\ \ 83\ \ 65 =$ 01010010 01010011 01000001 u ASCII kôdu.
- Alisa deli ovaj niz u dva 12-cifrena binarna broja **01010010**0101 0011**01000001** $= 1317\ \ 833 = M_1\ \ M_2$.
- Koristeći Bobov javni ključ $(n, e) = (4189, 671)$, Alisa računa

  $C_1 = M_1^e = 1317^{671} \equiv 3530 \pmod{4189}$
  $C_2 = M_2^e = 833^{671} \equiv 3050 \pmod{4189}$,

  i dobija šifrat:
- $C \equiv C_1\ \ C_2 \equiv 3530\ \ 3050 \equiv 0110111001010\ \ 0101111101010$.
- Alisa šalje Bobu šifrovanu poruku, binarni niz C.

RSA: Primer

Bob dekriptuje šifrovanu poruku C na sledeći način:

- Bob računa

  $M_1 = C_1^d = 3530^{1791} \equiv 1317 \,(\mathrm{mod}\, 4189),$
  $M_2 = C_2^d = 3050^{1791} \equiv 833 \,(\mathrm{mod}\, 4189),$

  odakle koristeći ASCII tablicu nalazi originalnu poruku:
- $P = M_1\ M_2 \equiv 1317\ 833 =$

  $$\mathbf{01010010}0101\ 0011\mathbf{01000001} =$$

  $$01010010\ 01010011\ 01000001 = \text{"RSA"}.$$

RSA: Kako razbiti kôd

2010. godine razbijen 768-bitni šifarski sistem RSA koji se inače do tada koristio u praksi.

U 2013. pojavile su se studije koje ukazuju kako razbiti 4096-bitni RSA sistem koristeći takozvanu akustičku kriptoanalizu.

Razvojem kvantnih računara, RSA postupak sa ključevima praktično bilo koje dužine moći će da se razbije u deliću sekunde.

Već danas, koristeći velike kapacitete distribuiranog izračnavanja, moguće je razbiti RSA postupak sa ključevima bilo koje dužine.