KRALJEVINA JUGOSLAVIJA

UPRAVA ZA ZAŠTITU INDUSTRISKE SVOJINE

Klasa 15 (5)

Izdan 1 septembra 1933.

PATENTNI SPIS BR. 10340

Prikelmajer Josif, apotekar, Valjevo, Jugoslavija.

Postupak i uredjaj za šifrovanje i dešifrovanje poverljivih sastava.

Prijava od 11 decembra 1931. Važi od 1 marta 1933.

Dosadašnji način šifrovanja poverljivih sastava pomoću rečnika snabdevenih brojnim oznakama za svaku reč ili za čitave rečenice ima svoju veliku nezgodu, što pri svakoj povredi tajne šifre, odnosno pri saznanju da je šifra dospela u neovlašćene ruke, mora da se pristupa menjanju celokupne šifre, što pričinjava velike neugodnosti i troškove. Osim toga dosadašnji način šifrovanja ima i tu nezgodu što pored lica kojem je šifrovani izveštaj ili naredenje upućen, isto mogu rastumačiti i ostala lica kojima je šifra poverena, a u dotični izveštaj ili naredenje ne bi trebalo da budu posvećena.

Ovim se pronalaskom izbegavaju sve nezgode dosadašnjeg načina šifrovanja izveštaja, a naročito ostaje zagarantovana tajna saopštenja, pošto se za svako lice može imati drugi ključ šifre, ili se i sa jednim i istim licem za razne datume ili nedeljne dane, dakle prema dogovoru o načinu sastavljanja šifrovanog sastava (izveštaja) mogu imati razni ključevi šifre, tako, da time dešifrovanje izvesne vesti postaje moguće samo od strane lica koje je direktno posvećeno u tajnu ključa za dotični sastav (vest).

Postupak po ovom pronalasku se sastoji u sledećem:

Svako slovo, odnosno pismeni znak, koji može biti i otkucan pomoću za ovo preudešene pisaće mašine, biva zamenjeno po jednim dvocifrenim brojem, tako na primer slovo W može biti zamenjeno brojem 63, ili proizvoljnim drugim brojem, koji se u šifrovanom sastavu može ispisati na više načina prema izboru i dogovoru, na primer $63, \frac{6}{3}, \frac{3}{6}$.

Radi lakšeg razumevanja pronalaska o vom opisu je priložen nacrt u kojem: sl. 1 pokazuje jedan oblik izvodenja azbučne tablice, sl. 2 pokazuje jedan oblik izvodenja tablice sa brojevima, sl. 3 pokazuje kombinaciju jednog reda iz azbučne tablice sa jednim redom iz tablice sa brojevima, sl. 4 pokazuje jedan oblik izvodenja tablice sa brojevima u primeni na valjku jednog od poznatih tipova pisaćih mašina, koje rade pomoću valjka za otiskivanje pismenih znakova, sl. 5 pokazuje jedan oblik izvodenja azbučne tablice opet na valjku pomenute pisaće mašine, koja služi za dešifrovanje sastava pomoću pisaće mašine, sl. 6 pokazuje jedan, pomerljivi red iz azbučne tablice koji je preudešen za rad pomoću pisaće mašine, i najzad sl. 7 pokazuje jedan primer redanja slobodno pomerljivih polja, na kojima se ispisuje šifrovani sastav radi daljeg planskog zamršivanja šifre.

U sl. 1 i 2 su pokazane dve tablice koje čine osnovu za izvodenje šifre po ovom pronalasku. Ove tablice imaju isti broj horizontalnih redova i isti broj vertikalnih redova, tako, da se na taj način dobija izvesan broj polja, ovde 84, od kojih svako polje u jednoj tablici sadrži izvesan pismle-

drugoj tablici svako polje sadrži izvesan dvocifreni broj, čije cifre mogu biti ispisivane na napred pomenute načine. Osim toga svako polje i u jednoj i u drugoj tablici dobija svoju oznaku horizontalnog reda na primer VI i oznaku mesta u horizontalnom redu, na primer 5, 4, 3 itd. Tako na primer polje u kome se nalazi slovo V ima svoje oznake VI, 9 čime se potpuno određuje položaj polja u tablici. Isti je slučaj i kod tablice čija polja sadrže dvocifrene brojeve, na pr. polje u kome se nalazi broj 73 obeleženo je sa IV, 2

Ako se sad ove tablice konstruktivno tako izvedu, da se horizontalni ili vertikalni redovi mogu pomerati levo ili desno, ili gore ili dole, dobija se mogućnost da izvesnom slovu odnosno polju u jednoj tablici može odgovarati proizvoljno polje iz odgovarajućeg reda u drugoj tablici. Ako se osim toga tablice još i tako konstruktivno izvedu da i horizontalni ili vertikalni redovi u tablicama mogu slobodno menjati svoja mesta, na primer da red I dospe na mesto reda VI, onda je jasno da izvesno slovo iz jedne tablice može biti zamenjeno proizvoljnim dvocifrenim brojem iz druge tablice.

Iz napred navedenog je jasno, da se izvesno saopštenje pomoću ovih dveju tablica može izvesti samo tako ako se dva lica, koja će se ovim tablicama služiti, dogovore o rasporedu slova i brojeva u tablicama, dalje ako ugovore ključ šifre. Ključ šifre se dobija, kod izdeljenosti tablice u horizontalne redove, čitanjem u vertikalnom redu oznaka polja. Za tablice u sl. 1 i 2 bi dakle ključevi i za jednu i za drugu tablicu glasili 5555555 sa normalnim radom horizontalnih redova I, II itd.

Ako zamislimo da je pomoću ugovorenih ključeva obrazovan izvestan raspored polja ovih tablica, to se sad može pristupiti ispisivanju, odnosno otkucavanju šifrovanog sastava. Ako pak postoje razlozi da se želi da se šifrovani sastav što je moguće više zamrsi i da se planski unište slova, to će se ovo ispisivanje izvesti na naročito predviđenim slobodno pomerljivim poljima 1 (sl. 7) u vidu okruglih četvrtastih pločica ili tela, koja mogu biti vođena i po vodiljama, i koja se postavljaju jedno do drugog, kao u sl. 7, da se dobijaju redovi polja slično šahovskoj tabli. Pri upisivanju dvocifrenih brojeva u ova polja, svako polje dobija po jednu cifru odgovarajućeg broja i to se upisivanje vrši po jednom od ugovorenih načina na primer $\frac{7}{3}$, ili $\frac{3}{7}$, ili 73 (vidi sl. 7).

Ako sad zamislimo da je na ovim poljima iz sl. 7 napisan izvesan izveštaj u šifri to ćemo prema načinu ispisivanja cifara u poljima pomenute tablice (na pr. 73, ili $\frac{3}{7}$, ili $\frac{7}{3}$) dobiti izvesan niz cifara, odnosno redove cifara. Pošto svakom slovu odnosno pismenu odgovara izvesan dvocifreni broj to nam je sad, kad je izveštaj napisan, moguće, da pomoću novog ili istog ključa proizvedemo željeni novi razmeštaj cifara, t. j. da cifre svih dvocifrenih brojeva rastavimo i da ih pomerimo za nekoliko mesta dalje od njihovog prvobitnog mesta. Kod načina upisivanja cifara u polja, na tablici po sl. 7, jedne pored druge (na pr. 73) pomeranje cifara bi se izvelo prvo u vertikalnim linijama, a kod načina ispisivanja cifara jedne iznad ili ispod druge (na pr. $\frac{7}{3}$, ili $\frac{7}{3}$), pomeranje bi se izvelo najpre u horizontalnim redovima. Ovim rastavljanjem i pomeranjem cifara se proizvodi željeno potpuno uništavanje brojeva koji pretstavljaju slova iz prve tablice. Da bi se postigla još veća zamršenost slova cifara to se kod prvog slučaja (cifre 73) posle pomeranja vertikalnih redova vrši i pomeranje horizontalnih redova za nekoliko mesta levo ili desno, ili u drugom slučaju (cifre $\frac{3}{7}$, ili $\frac{7}{3}$) pomeranje vertikalnih redova za nekoliko mesta gore ili dole.

Kao što se iz napred navedenog vidi, dvocifreni, odnosno višecifreni brojevi su predviđeni kao zamene pojedinih slova (pismena, znakova) jedino u cilju postizanja mogućnosti što potpunijeg zamršivanja slova, tako, da se ni po kojoj metodi računa verovatnoće ne može izvršiti dešifrovanje izvesnog izveštaja. Iz prednjeg opisa je jasno da po ovom postupku šifrovani izveštaj može biti dešifrovan samo od strane lica koje je direktno posvećeno u ključeve i u red kojim se vršilo šifrovanje, a koje po dobitku šifrovanog izveštaja pristupa obrnutim redom dešifrovanju.

Naprava za izvođenje ovog postupka može biti izvedena prosto iz dveju gore navedenih tablica, koje su tako udešene da se horizontalni redovi mogu premeštati iz nižeg u viši red i obratno, odnosno da se po želji mogu kombinovati redovi slova sa redovima cifara, tako, da se iznad ili ispod svakog slova (pismenog znaka) može odmah očitati dvocifreni broj koji za dotičnu šifru ovom slovu odgovara ili obratno (vidi sl. 3).

U slučaju da se šifrovanje želi da vrši pomoću pisaće mašine, to se za ovo uređaj može najpovoljnije izvesti preuređenjem već poznatih tipova pisaćih mašina, koje za otkucavanje sadrže naročiti valjak, koji se namiče na odgovarajuće vreteno. Ovo

se preudešavanje pisaćih mašina radi izvođenja postupka po ovom pronalasku može izvesti na više načina od kojih radi primera navodimo sledeći:

Kod poznatog tipa pisaće mašine na primer kod tipa »Mignon« (koju izrađuje firma A. E. G.), azbučna tablica biva zamenjena tablicom na primer iz sl. 1 (sam mehanizam pisaće mašine nije pretstavljen, pošto se smatra kao poznat i nepotreban po razumevanje pronalaska). Tablica se i ovde deli u odgovarajući broj pokretnih redova, koji se izvode iz beskonačnih traka 2 (sl. 6), koje se mogu pokretati preko valjaka 3 postavljenih sa strane, pri čemu su na ovim trakama ispisani pismeni znaci sa svojim odrednim oznakama. Radi primera je pokazana jedna takva traka u sl. 6. Ove trake nose dva ili više puta ponovljeno ispisani red oznaka tako, da se pri pomeranju traka brojevi koji zalaze na jednoj strani jednovremeno javljaju na drugoj strani.

Napred opisanoj tablici odgovara valjak iz sl. 4, na kojem se nalaze dvocifreni brojevi koji treba da zamene slova (pismene znake). Ovaj valjak je izdeljen u veći broj prstenova 4 tako, da svaki prsten na svojim ispupčenjima 5 nosi dvocifrene brojeve slično horizontalnim redovima dvocifrenih brojeva iz tablice iz sl. 2. Osim toga svaki prsten nosi svoju oznaku reda na primer I, II, itd. a pored svakog broja u udubljenju 6 se postavlja oznaka koja određuje mesto slova u redu, odnosno ovde u prstenu. Svaki prsten se osim toga snabdeva vodiljnim žljebom koji nije pokazan, tako, da se prema početnoj oznaci na vretenu 8 koje nosi valjak može podesiti proizvoljan broj sa dotičnog prstena.

Ako se kod napred navedenog rada pomoću pisaće mašine želi da izvede dalje zamršivanje, to se ispod hartije na kojoj se otkucava izveštaj postavlja indigo namazanom stranom prema poleđini hartije tako da se ne mora vršiti prepisivanje na slobodna polja, već se na ova polja prosto pritiskom prenosi otisak slova sa poleđine hartije, posle čega se zamršivanje izvodi na već opisani način.

Za izvođenje dešifrovanja pomoću pisaće mašine, predviđa se još jedna garnitura tablice i odgovarajućeg valjka, pri čemu sad tablica nosi brojeve iz tablice prema sl. 2, a valjak nosi pismena (slova) iz tablice prema sl. 1. Valjak za izvođenje dešifrovanja se inače tako sastoji iz pokretnih prstenova 4 kao i valjak sa brojevima, a pokazan je na sl. 5.

Patentni zahtevi:

1. Postupak za šifrovanje naznačen time, što se pojedina slova azbuke (pismeni znaci) zamenjuju dvocifrenim, odnosno višecifrenim brojevima, koji se po izvedenom šifrovanom sastavu planski uništavaju pomoću ugovorenog razmicanja i pomeranja cifara, koje sačinjavaju ove brojeve, za izvesan broj mesta u vertikalnim i horizontalnim redovima, pri čemu se, prema načinu upisivanja cifara u slobodno pokretna polja, ili prvo vrši pomeranje vertikalnih redova, ili se pak vrši prvo horizontalno a zatim vertikalno pomeranje pomenutih redova cifara.

2. Postupak za izvođenje šifrovanih sastava po zahtevu 1, naznačen time, što se za ispisivanje šifrovanog sastava predviđa veći broj pokretnih, okruglih, četvrtastih ili t. sl., polja, koja se postavljaju jedno do drugog tako, da se približno dobija izgled polja šahovske table, pri čemu svako polje dobija samo po jednu cifru dvocifrenog, odnosno višecifrenog broja, tako, da se po izvršenom upisivanju šifrovanog sastava može preduzeti pomeranje vertikalnih i horizontalnih redova ovih polja, po izvesnom planu, odnosno dogovoru, radi razmicanja odnosno uništavanja brojeva koji pretstavijaju slova, odn. pismene znake.

3. Uređaj za izvođenje postupka po zahtevu 1 i 2, naznačen time, što je kod jednog od poznatih tipova pisaćih mašina, na primer kod pisaće mašine »Mignon« reljefni valjak, koji sadrži slova za otkucavanje, zamenjen odgovarajućim brojem reljefnih prstenova (4), koji, svaki, sadrži dvocifrene brojeve, i koji se po volji mogu tako podešavati i fiksirati na vretenu koje nosi pomenute prstenove, da izvesnom slovu sa azbučne table odgovara željeni broj ili obratno.

4. Uređaj po zahtevu 3, naznačen time, što svakom pokretnom reljefnom prstenu koji nosi brojeve (slova) odgovara red slova (brojeva) na azbučnoj tablici, koji se takođe može podešavati pomeranjem u jednom ili u drugom smeru.

—	№	*	9	8	7	6	5	4	3	2	1
*	X	L	O	W	P	O	U	V	Z	H	Q
,	E	M	У	N	I	L	C	A	E	T	G
.	S	R	H	A	E	T	O	S	R	F	M
!	D	A	E	T	S	D	N	I	N	L	I
=	I	F	N	C	R	A	E	T	O	S	B
§	*	.	”	:	,	*	?	*	;	K	J

Sl. 1

92	84	77	69	62	55	47	40	33	25	18	11
93	85	78	71	63	56	48	41	34	26	19	12
94	86	79	72	64	57	49	42	35	27	20	13
95	87	80	73	65	58	51	43	36	28	21	14
96	88	81	74	66	59	52	44	37	29	22	15
97	89	82	75	67	60	53	45	38	31	23	16
98	91	83	76	68	61	54	46	39	32	24	17

Sl. 2

8	41	34	26	19	12	93	85	78	71	63	56	48	41	34	26	19	12
	!	D	A	E	T	S	D	N	I	N	L	I	!	D	A	E	T	S	D

Sl. 3

—	№	*	9	8	7	6	5	4	3	2	1
*	X	J	O	W	P	O	U	V	Z	H	G
»	E	M	Y	N	I	L	C	A	E	T	G
«	S	R	H	A	E	T	O	S	R	F	M
!	D	A	E	T	S	D	N	J	N	L	I
–	I	F	N	C	R	A	E	T	O	S	B
§	*	-	"	:	?	*	?	*	;	K	J

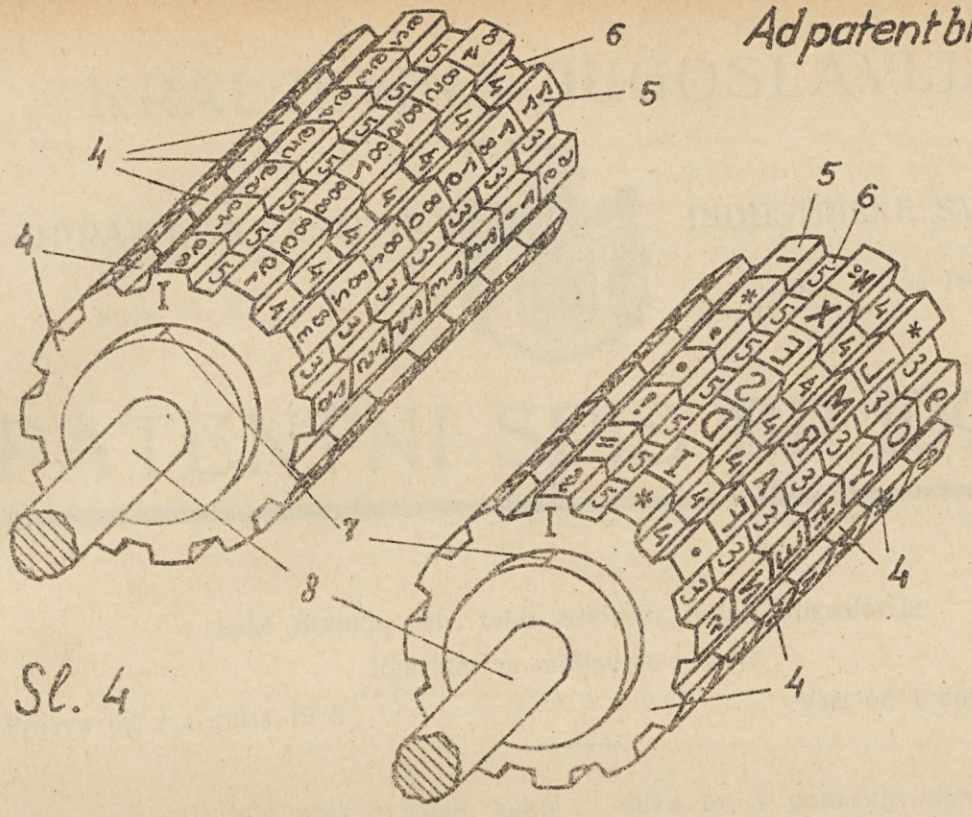
SL.1

92	84	71	69	62	55	47	40	33	25	18	11
93	85	78	71	63	56	48	41	34	26	19	12
94	86	79	72	64	57	49	42	35	27	20	13
95	87	80	73	65	58	51	43	36	28	21	14
96	88	81	74	66	59	52	44	37	29	22	15
97	89	82	75	67	60	53	45	38	31	23	16
98	91	83	76	68	61	54	46	39	32	24	17

SL.2

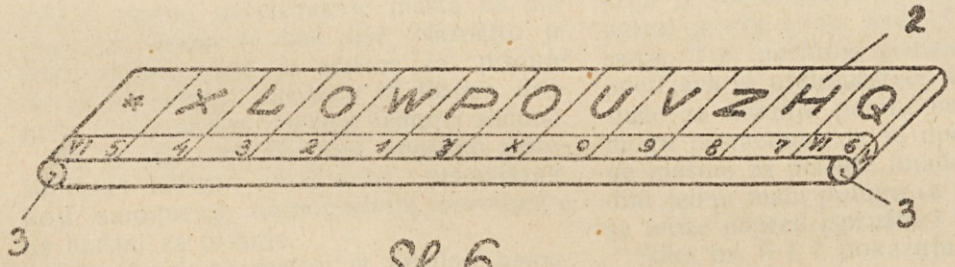
8	41	34	26	19	12	93	85	78	71	63	56	48	41	34	26	19	12							
!	D	A	E	I	S	D	N	I	N	L	!	!	I	D	A	E	T	S	D					

SL.3

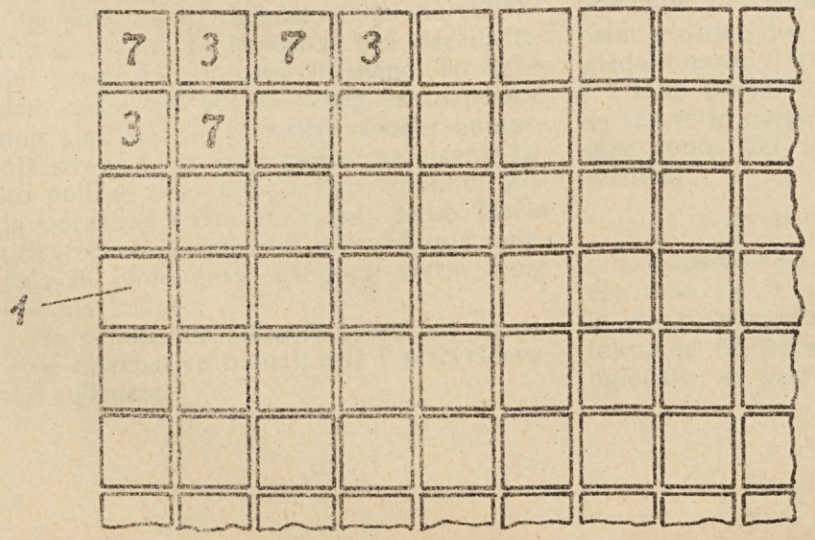


Sl. 4

Sl. 5



Sl. 6



Sl. 7