Domaci 3 - kriptografija

Ognjen Čavić E2 161/2024

Novembar 2024

1 Prvi zadatak

Prvi zadatak je šifrovati frazu **VENI VIDI VICI** pomoću *Playfair* algoritma. Ponuđeni ključevi, tj reči kojima se matrica (ili tabela) slova može pomešati, su **IRITIRATI**, **ANANAS** i **SUNCE**. U opštem slučaju, cilj je da se za ključ odabere reč sa što više različitih slova jer to rezultuje tabelom koja je više izmešana. Stoga je najbolja reč od ponuđenih **SUNCE** jer ima najviše različitih slova čak iako je najkraća i time se dobija najmanje predvidiva tabela.

S	U	N	C	E
A	B	D	F	G
H	I	K	L	M
O	P	Q	R	T
V	W	X	Y	Z

Tabela 1: Matrica slova *Playfair* algoritma kada se koristi reč **SUNCE**

Nakon što se fraza podeli u segmente od po dva slova koji se šifruju na osnovu matrice, dobija se konačna poruka:

Segmenti originalne poruke	VE	NI	VI	DI	VI	CI
Segmenti šifrovane poruke	ZS	UK	WH	BK	WH	UL

Tabela 2: Odgovarajući segmenti šifrovane i originalne poruke

koja glasi **ZSUKWHBKWHUL**.

2 Drugi zadatak

Dok se prvi zadatak bavio šifrovanjem poruke, cilj drugog jeste da dešifruje primljenu poruku ukoliko je ključ poznat. Dodatna komplikacija je to što koristi ćirilično pismo, koja sadrži 30 slova i zahteva produženje tabele. Fraza koju treba dešifrovati je **ОЗМЕЖАУЛМОЛИЛППНХОЏ** dok ključ koji se koristi je **КОЛОКВИЈУМ** i nakon uklanjanja svih slova koja se ponavljaju dobija se **КОЛВИЈУМ**. Na osnovu ključa se formira matrica slova.

К	О	Л	В	И	Ј
У	М	А	Б	Г	Д
Ђ	Е	Ж	З	Љ	Н
Њ	П	Р	С	Т	Ћ
Ф	Х	Ц	Ч	Џ	Ш

Tabela 3: Tabela *Playfair* algortima za ćirilična slova

Postupak dešifrovanja je isti kao i postupak šifrovanja sa tim da za slova u istom redu ili koloni pomera se ulevo umesto udesno i na gore umesto na dole, respektivno. Nakon što je sve potrebno za dešifrovanje poznato, preostaje samo to i odraditi:

Segmenti šifrovane poruke	ОЗ	МЕ	ЖА	УЛ	МО	ЛИ	ЛП	НХ	ОЏ
Segmenti dešifrovane poruke	ВЕ	ОМ	АЛ	АК	ОХ	ОВ	ОР	ЕШ	ИХ

Tabela 4: Odgovarajući segmenti šifrovane i originalne poruke

nakon odbacivanja obojenog **Х** koje je umetnuto kako bi se izbeglo da se dva ista slova nalaze u segmentu, dobija se konačna poruka **ВЕОМА ЛАКО ОВО РЕШИХ**.