Playfairova sifra

1. Preskačemo jedan karakter kako bi imali matricu 5x5
2. Poruku sifriramo tako sto karaktere odvajamo na parove (2 karaktera).
   Pravila:
1. Ukoliko se dva karatera nađu **u istoj koloni**, njihove vrednosti se zamenjuju karakterima ispod njih.
2. Ukoliko se dva karaktera nađu **u istom redu**, njihove vrednosti se zamenjuju prvim karakterima sa njihove desne strane.
3. Ukoliko se dva karaktera nađu **na različitim mestima**, formiraćemo kutiju (pravougaonog ili kvadratnog oblika) od karaktera sa kojima treba da ih zamenimo – menja se krajnjim desnim karakterom.
4. Ukoliko nam **fali jedan karakter**, dodajemo karakter **X**.
5. Ukoliko imamo **par istih karaktera**, drugi karakter menjamo karakterom **X**.
6. Slova I i J se poistovećuju

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

Primer 1. Upotrebom Playfairovog algoritma šifrovati sledeću poruku.

Poruka: “Ovu poruku treba siftovati danas”

Korak 1: Napravimo string: O V U P O R U K U T R E B A S I F R O V A T I D A N A S

Korak 2: Odvojimo karaktere: **OV UP OR UK UT RE BA SI FR OV AT ID AN AS**

Korak 3: Formirajmo kolone, redove i kutije.

Korak 4: Sifrovana poruka: **LY ZU MT ZP QU UB CB TH GQ LY DQ OI CL CQ**

2. Upotrebom Playfairovog algoritma šifrirati sledeću poruku:
Poruka: „DANAS POLAZEM DRUGI KOLOKVIJUM IZ PREDMETA ZASTITA PODATAKA“

DA	NA	SP	OL	AZ	EM	DR	UG	IK	OL	OK	VI	JU	MI	ZP	RE	DM	ET	AZ	AS	TI	TA	PO	DA	TA	KA	
AB	LC	UN	LM	EV	BP	BT	RK	KF	LM	PI	YF	KT	OG	EU	UB	BO	DU	EV	CQ	YO	QD	LP	EB	QD	FE	

3. Upotrebom Playfairovog algoritma i tabele iz prethodnog zadatka izvršiti dekripciju sledeće poruke:
Poruka: „NPYEC QBL LPMPYKT ISQHK IPMPFZPPRP KY MUAEPBQD EUGP“

NP	YE	CQ	BL	LP	MP	YK	TI	SQ	HK	IP	MP	FZ	PP	RP	KY	MU	AE	PB	QD	EU	GP			
MO	ZD	AS	AM	PO	LO	ZI	OD	RU	GI	KO	LO	KV	IJ	UM	IZ	PR	ED	ME	TA	ZP	KM			

4. Šifrirati otvoreni tekst CRYPTOGRAPHY pomoću Playfairove šifre sa ključem ***PLAYFAIR***.

Ovde unosimo u tabelu reč Playfair ali vodimo računa da se slova ne ponavljaju. Nakon toga popunjavamo alfabet sa preostalim slovima koja fale u tabeli.

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

CR	YP	TO	GR	AP	HY
DB	FL	NQ	OG	YL	KA

5. Šifrirati otvoreni tekst NAPADAMO U PODNE AKO NE BUDE VETRA pomoću Playfairove šifre sa ključem ***VETROBRAN***

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

na pa da mo up od ne ak on eb ud ev et ra

cn mn bn se xl dk at dg td va zb te tr ec