Fakultet Informatike u Puli

Playfairova šifra

Napravili: Antonio Jadrejčić i Gregor Kostić

Povijest

- Playfairovu šifru je izumio **Charles Wheatstone.**
- Ona je dobila ime po njegovom prijatelju **Lord Lyon Playfairu** koji ju je popularizirao.
- Prvi zabilježeni opis Playfair šifre nalazi se u dokumentu koji je potpisao Wheatstone 26. ožujka 1854.

Charles Wheatstone

Lord Lyon Playfair

Povijest

Koristila ga je britanska vojska u Drugom burskom ratu i Prvom svjetskom ratu u taktičke svrhe.

Iz istog razloga su je koristili Britanci i Australci tijekom Drugog svjetskog rata.

Jako je bila brza za korištenje, te nije zahtijevala nikakvu posebnu opremu.

Tijekom Drugog svjetskog rata vlada Novog Zelanda ga je koristila za komunikaciju između Novog Zelanda, Chatamskih otoka i promatrača obale na pacifičkim otocima.

Sadašnjost

- Playfair više ne koriste vojne snage zbog pojave digitalnih uređaja za šifriranje.

- Ova šifra se sada smatra nesigurnom za bilo koju svrhu, jer bi je moderna računala mogla lako razbiti unutar nekoliko mikrosekundi.

- Playfairova šifra je **bigramska šifra** (šifriraju se parovi slova i to na način da rezultat ovisi i o jednom i o drugom slovu).
- Algoritam za šifriranje se bazira na 5x5 matrici slova, koja se konstruira koristeći ključnu riječ. U našem slučaju ključna riječ će biti '**Keyword**'.
- Engleska abeceda ima 26 slova iz kojeg razloga je da se slova I i J poistovjete.

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

Pravila za stvaranje tablice

- 1. Stavi slovo I i J u istu ćeliju
- 2. Stavi željenu riječ u tablicu (Keyword)
- 3. Ostala slova nakon odabrane riječi idu abecednim redom

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

Pravila pripremanja poruke

- Slova moraju biti podijeljene u parove
- Sve duplikate odvajamo stavljajući slovo x između njih
- Ako je zadnje slovo neparno onda dodajemo slovo x na kraju.
- Ignoriramo sve razmake

Naša poruka bi onda bila SECRET MESSAGE.

SE CR ET ME SX SA GE

Pravila za dešifriranje

- Svaki par poruke stavimo u posebnu odvojenu tablicu
- 1. Ako su u istom stupcu:
  - Svako slovo pomaknuti za 1 dolje
- 2. Ako su u istom redu:
  - Svako slovo pomaknuti za 1 udesno
- 3. Ako se formiraju slova u obliku pravokutnika
  - Zamijeni slova sa onima na kraju pravokutnika

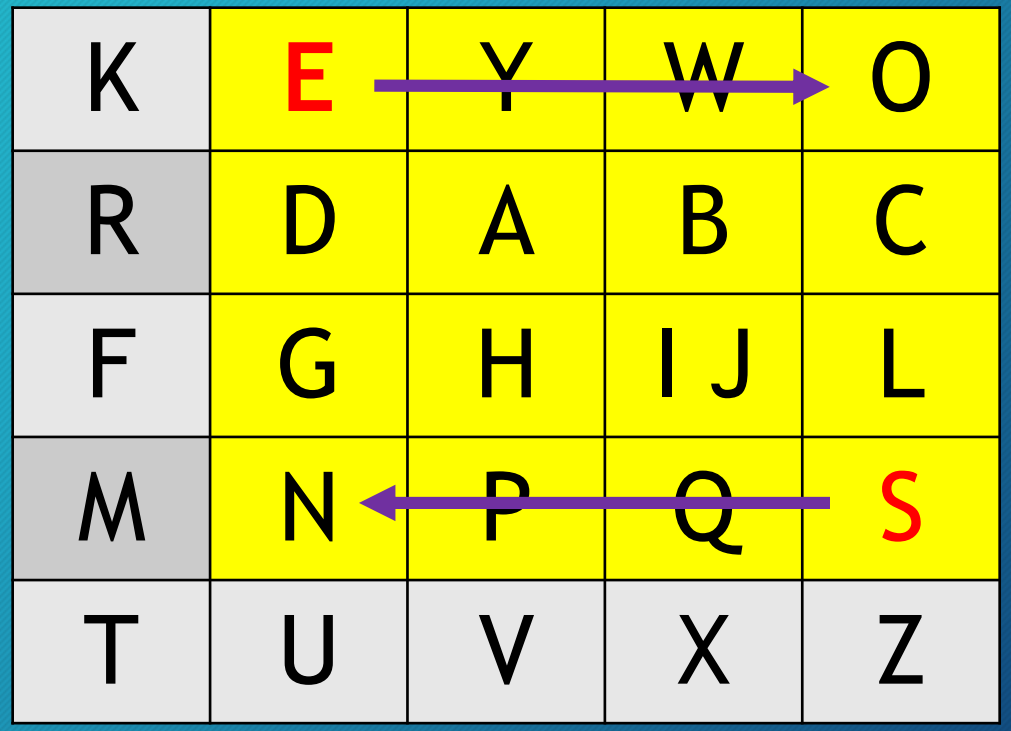
SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE



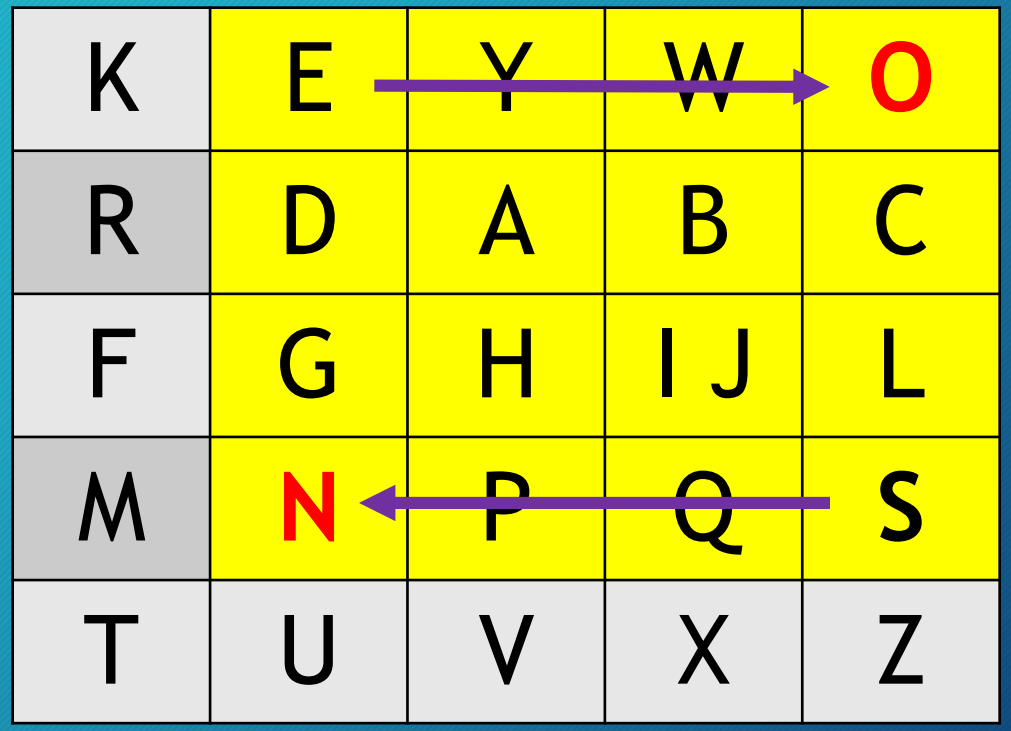
SE CR ET ME SX SA GE

- Prvi dekodirani tekst:

  NO

Dekodirani tekst:

NO



SE CR ET ME SX SA GE

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

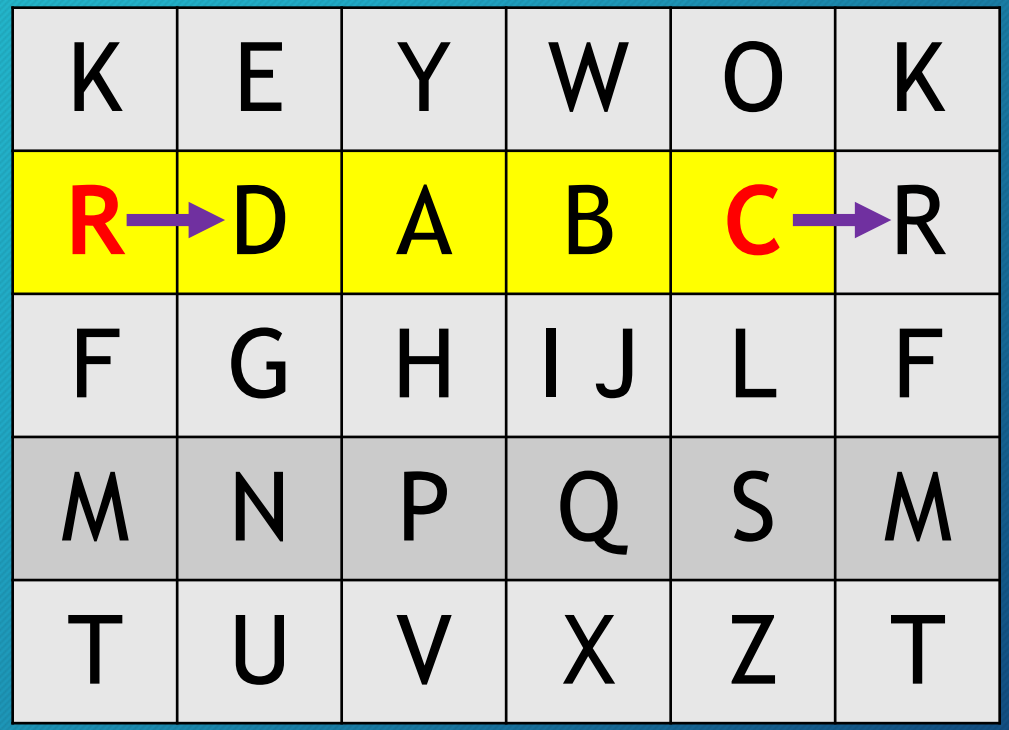
SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE



SE CR ET ME SX SA GE

- Drugi dekodirani tekst:

  RD

Dekodirani tekst:

NO RD

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

- Treći dekodirani tekst:

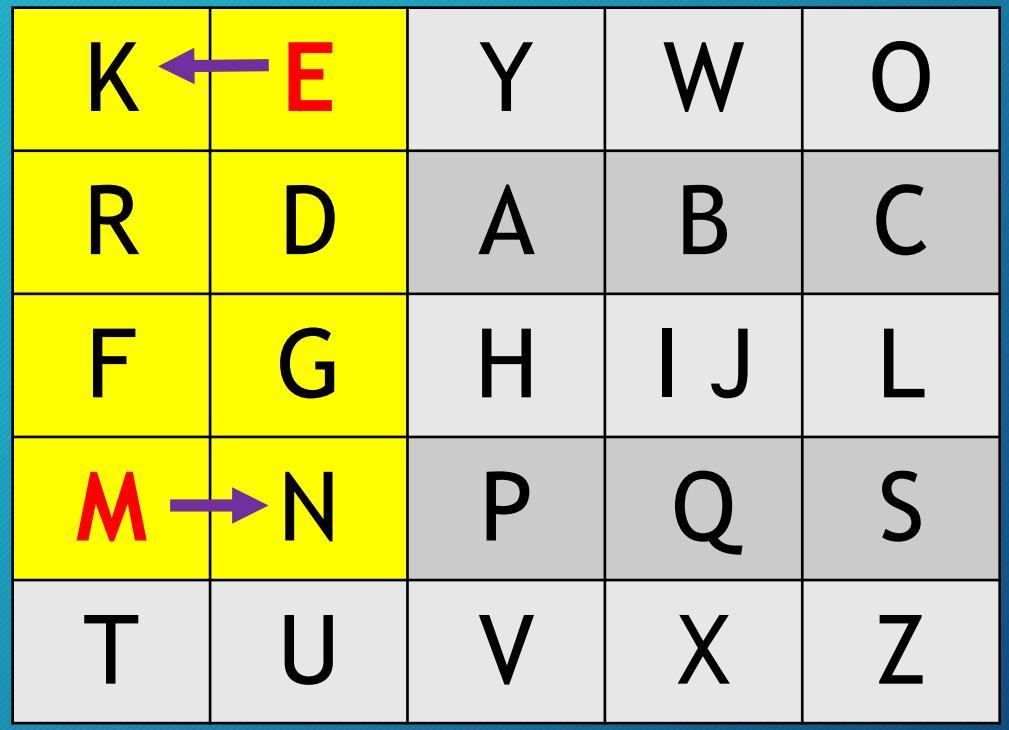
  KU

Dekodirani tekst:

NO RD KU

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

SE CR ET **ME** SX SA GE



SE CR ET ME SX SA GE

- Četvrti dekodirani tekst:

  NK

Dekodirani tekst:

NO RD KU NK

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

- Peti dekodirani tekst:

  QZ

Dekodirani tekst:

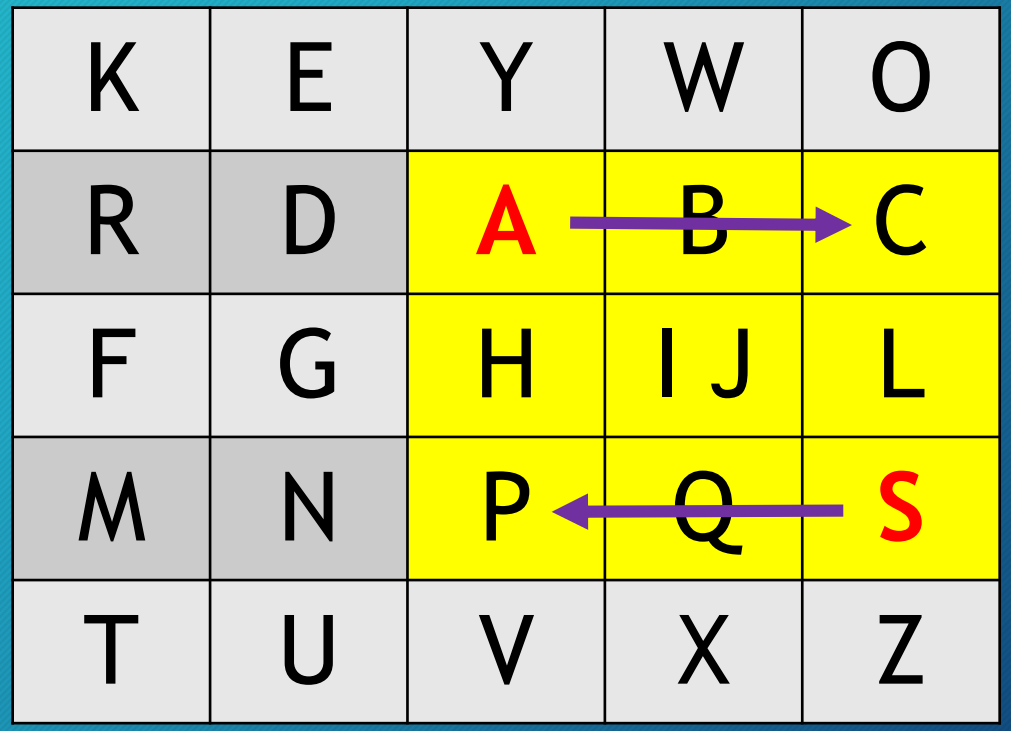
NO RD KU NK QZ

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE



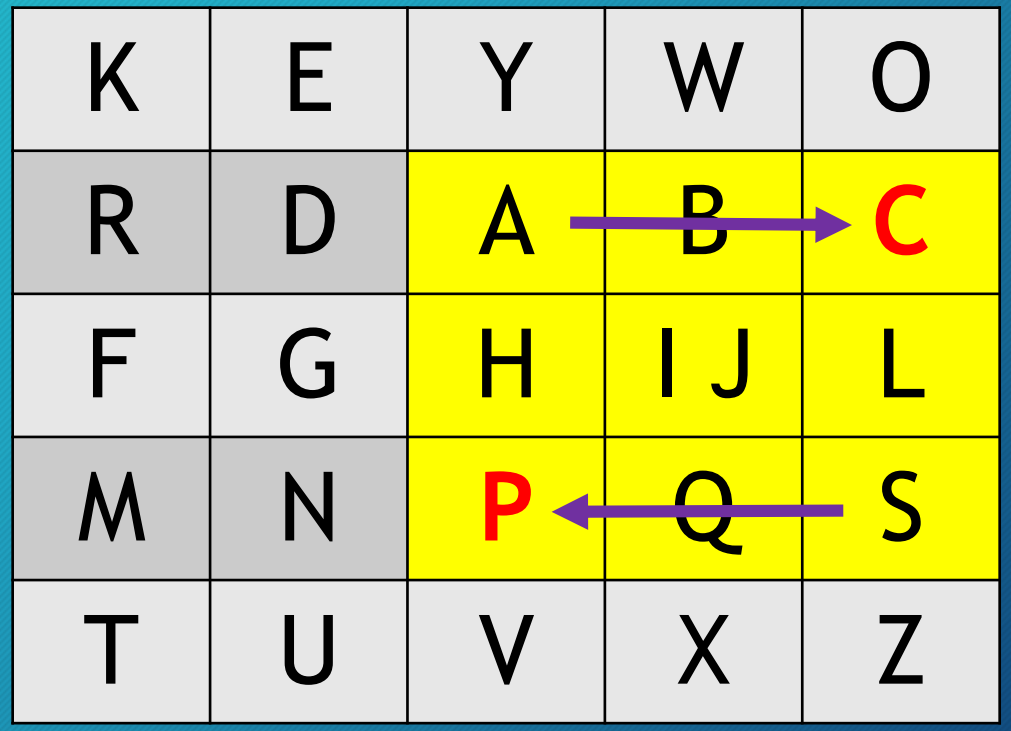
SE CR ET ME SX SA GE

- Šesti dekodirani tekst:

  PC

Dekodirani tekst:

NO RD KU NK QZ PC



SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

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

SE CR ET ME SX SA GE

- Posljedni dekodirani tekst:

  ND

Dekodirani tekst:

NO RD KU NK QZ PC ND

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

Literatura:

- Helen Fouche Gaines : Cryptanalysis a study of ciphers and their solution - https://archive.org/details/cryptanalysis00hele/mode/2up
- https://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html
- https://web.math.pmf.unizg.hr/~duje/kript/playfair.html
- https://www.javatpoint.com/playfair-cipher-program-in-java