Modulární systém dalšího vzdělávání pedagogických pracovníků JmK v přírodních vědách a informatice
CZ.1.07/1.3.10/02.0024

Klasické šifry – princip substituce, transpozice

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Základní principy šifrování

- Substituce
  - Nahrazení písmen za jiná
- Transpozice
  - Změna pořadí písmen

Základní substituce

- Monoalfabetická
- Každé písmeno se zobrazuje na jiné písmeno
- Pokaždé stejné

- Obecná substituce

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
P	E	Q	K	X	J	B	F	C	W	N	S	I	U	V	O	Z	M	A	D	Y	T	R	H	G	L

Základní substituce

- ATBASH

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

- Ceasarova šifra (posun o 3)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Základní substituce

- Substituce nastartovaná klíčem

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	A	J	N	Y	K	L	I	C	B	D	E	F	G	H	M	O	P	Q	R	S	U	V	W	X	Z

Lineární transformace

- Lineární transformace ax + b mod 26, x je pořadí písmena v abecedě, a,b jsou přirozená čísla, a je nesoudělné s 26
  - Zobrazení je jednoznačné – žádná dvě různá písmena se nezobrazí na to stejné
- Modulo:
  - mod
  - operace zbytek po dělení

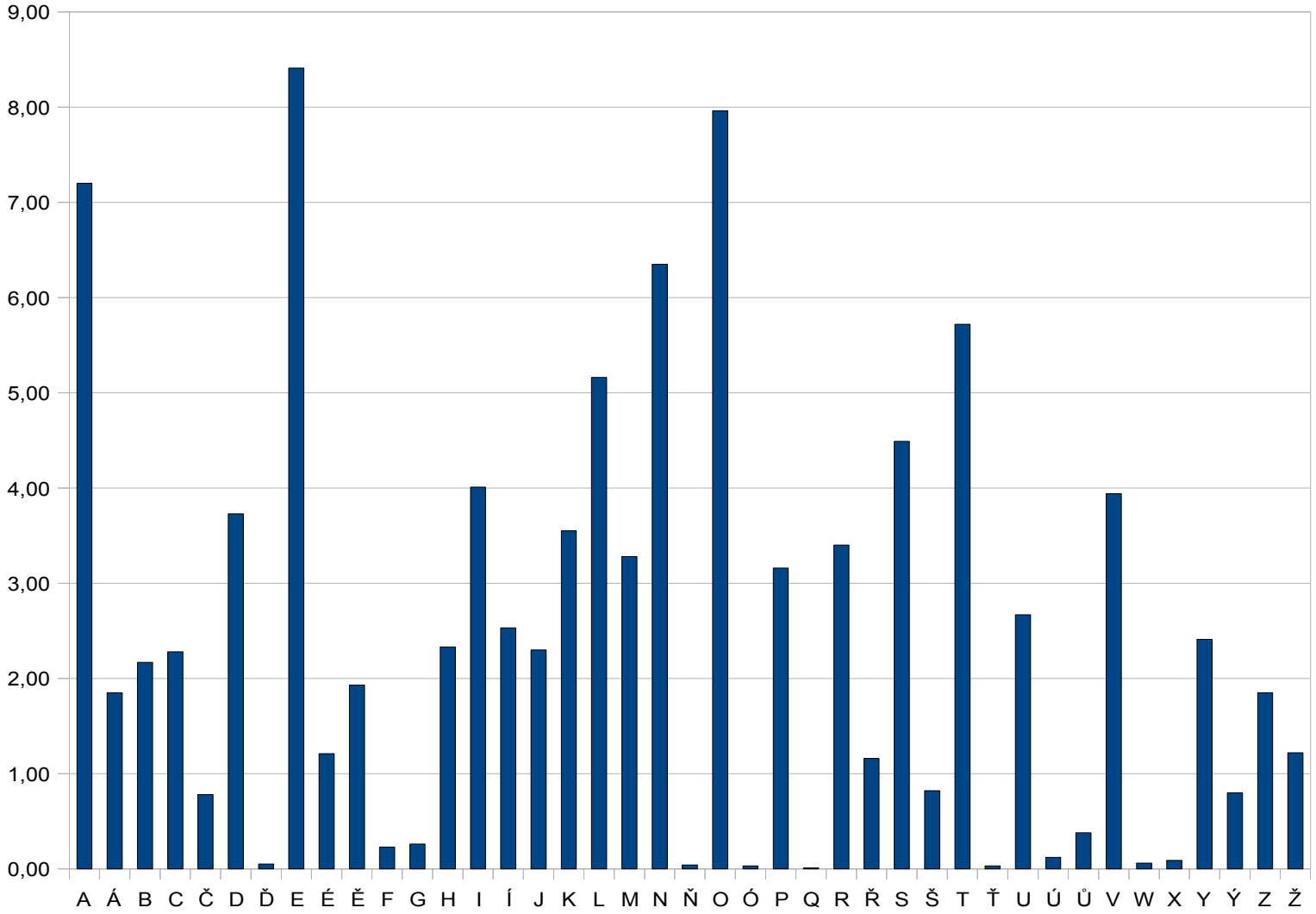
Jak na to?

- Hrubá síla?
  - 26! možností
  - ještě mnohem víc než miliarda miliard možností

Jak na to?

- Frekvenční analýza – statistická metoda
  - Některá písmena se v jazyce vyskytují častěji než jiná
  - Četnost písmen
  - Další charakteristiky jazyka: nejčastější slova, nejčastější začátky a konce,....
  - Monoalfabetické substituce jsou snadno rozluštitelné

Frekvenční analýza - histogram



Polyalfabetická substituce

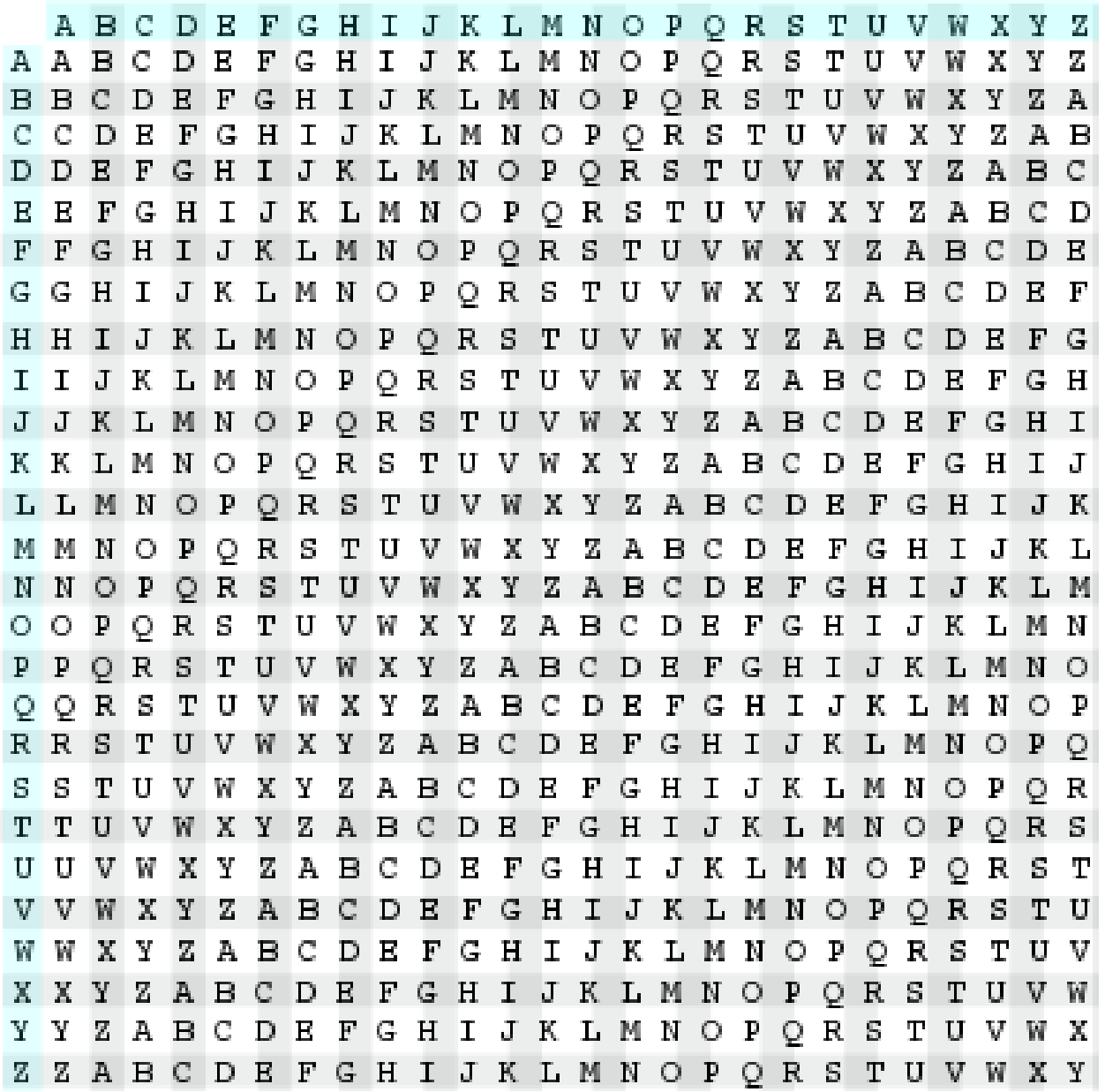
- Písmeno se zobrazuje na různá písmena v závislosti na jeho poloze v textu

Vigenérova šifra

- Kombinace Ceasarových šifer
  - Různé posuny
  - Pamatování posunů pomocí hesla – klíče
  - Sčítání písmen
    - a+a = a, a+b = b, b+b = c, m+b=o, m+c = p
    - co s tím, když to přeteče až za 'z'? modulo 26

c	o	j	e	s	e	p	t	e	m	t	o	j	e	c	e	r	t	e	m
t	a	j	n	y	k	l	i	c	t	a	j	n	y	k	l	i	c	t	a
V	O	S	R	R	O	A	B	G	F	T	X	W	C	M	P	Z	V	X	M

Vigenérův čtverec



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

Kryptoanalýza Vigenérovy šifry

- Ani Vigenérova šifra není nerozluštitelná
- Slabina: opakování klíče
- Známá délka klíče: frekvenční analýza
- Neznámá délka klíče:
  - Odhad shluků písmen.
  - Dva stejné řetězce pravděpodobně odpovídají stejným částem textu
- Čím delší klíč tím silnější

Bezpečnější varianty

- Klíč jen k nastartování, pak podle sebe sama

c	o	j	e	s	e	p	t	e	m	t	o	j	e	c	e	r	t	e	m
t	a	j	n	y	k	l	i	c	c	o	j	e	s	e	p	t	e	m	t
V	O	S	R	R	O	A	B	G	O	I	X	N	W	G	T	K	X	Q	G

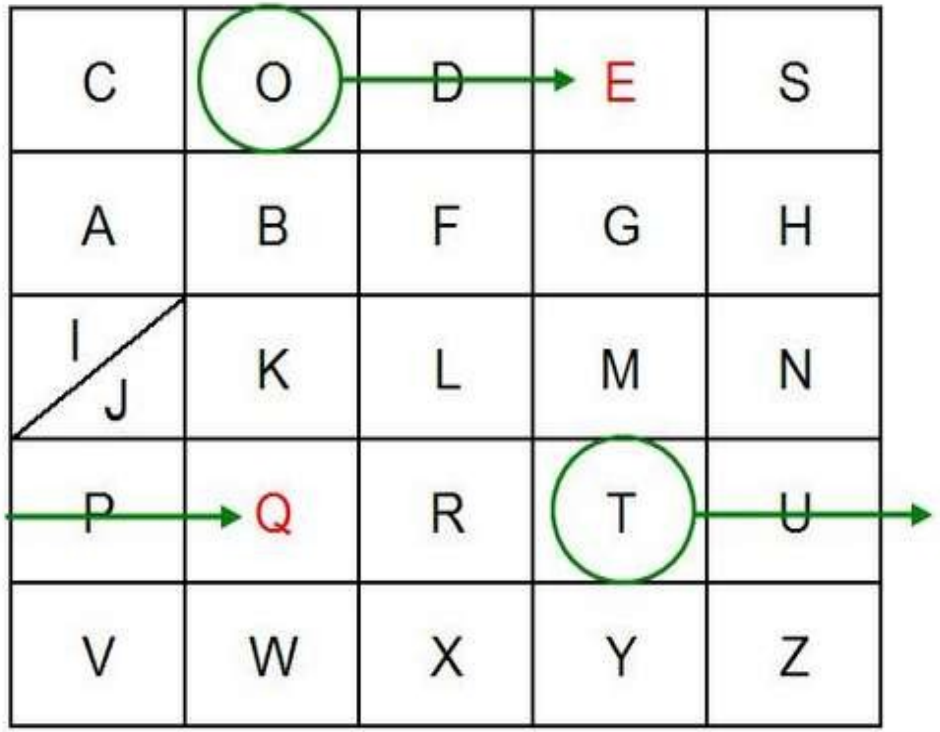
- Nejbezpečnější
  - klíč stejně dlouhý jako zpráva sama
  - použití klíče jen jednou
  - jednorázová tabulka (one-time pad)
  - problém: předání klíče mezi Alicí a Bobem

Polygrafické substituce

- Substituce ne na jedno písmeno, ale na celý blok

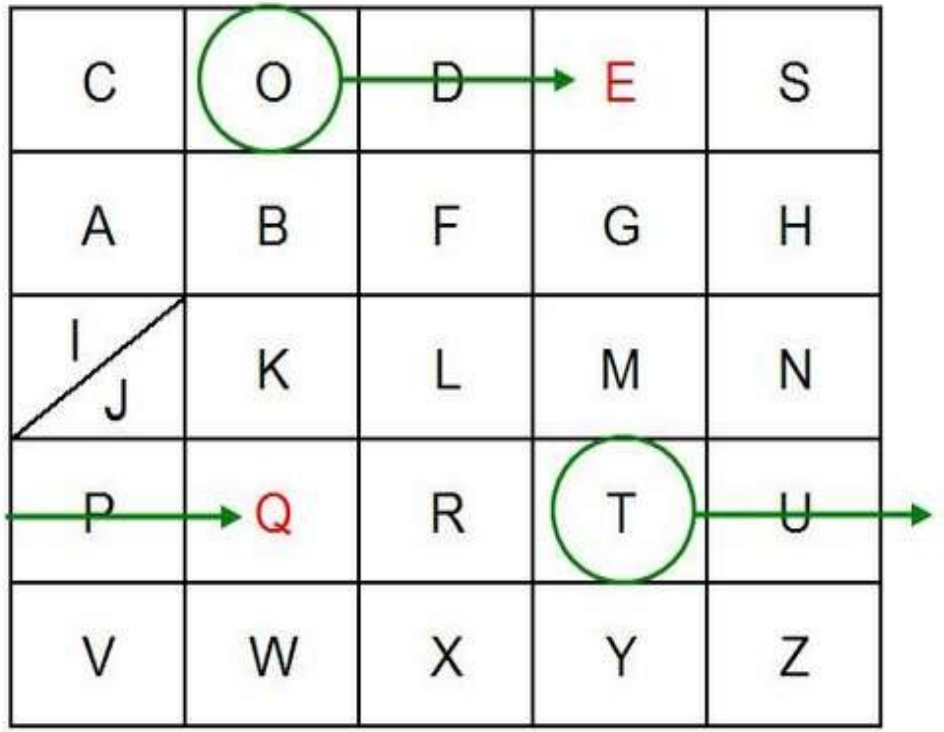
Playfair

- Dvojice písmen:
  - Stejný sloupec – nahraď obě o jedna dolů
  - Stejný řádek – nahraď obě o jedna do prava
  - Různý řádek i sloupec – nahraď druhými rohy čtverce



Playfair

- co → OD
- je → MC
- se → CS
- pt → QU
- em → GT



Jednoduchá transpozice

- Mění pořadí písmen
- Často geometrický princip
  - Coj Eš Epte Mto Ječ Er TeM
  - METREČ EJ OT METPEŠ EJ OC
  - COJEŠEPTEM

    TOJEČERTEM → CTOOJ JEEŠČ EEPRT TEEMM
  - CJŠPETJČRE

    OEETMOEETM → CJŠPE TJČRE OEETM OEETM

Složitější transpozice

- Tabulky – zápis podle systému, čtení po řádcích

E	Š	E	P	T
J	E	R	T	E
O	Č	M	E	M
C	E	J	O	T

- Spirála
  - EŠEPT JERTE OČMEM CEJOT

C	Š	E	J	R
O	E	M	E	T
J	P	T	Č	E
E	T	O	E	M

- Cik cak
  - CŠEJR OEMET JPTČE ETOEM

Transpozice podle klíče

H	E	S	L	O
C	O	J	E	Š
E	P	T	E	M
T	O	J	E	Č
E	R	T	E	M

E	H	L	O	S
O	C	E	Š	J
P	E	E	M	T
O	T	E	Č	J
R	E	E	M	T