EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Klasická kryptografie: Substituční šifry I

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Doc. Ing. Roman Šenkeřík, Ph.D. FAI,
Ústav informatiky a umělé inteligence

Obsah prezentace

- Monoalfabetické šifry.
  - Pevný posun
  - Reverzní abeceda (ATBASH)
  - Náhodná abeceda
  - Lineární posun
  - Substituce s klíčovým slovem
- Polyalfabetické šifry.
  - Vigenerova šifra
- Homofonní substituční šifry.
- Další přístupy pro ztížení prolomení substitučních šifer.

1. Monoalfabetické šifry

Monoalfabetické šifry: Pevný posun

Např. **Caesarova šifra** – příklad dle [1]

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

- Posun (rotace) abecedy o zvolený počet míst (1-25).
  - Caesarova pouze o 3.
- Alternativně lze zahrnout do „utajení“ i směr rotace abecedy.
- **Klíčem** je tedy velikost posunu – *d* a směr rotace.
- Pozor – nezaměnit s transpoziční šifrou – sice se jedná o posun, nikoliv ale o transpozici znaků v textu, nýbrž v rámci substituční abecedy.

Monoalfabetické šifry: Pevný posun

- Šifry jsou označovány jako ROT(*d*), tedy Caesarova šifra je ROT3
- Velmi známým dalším příkladem je šifra ROT13 – dochází zde k zrcadlení abecedy.

Algoritmizace šifry:

- Převedeme znaky na indexy 0 – 25 a aplikujeme jednoduchý vztah: (znak +*d*) mod 26.
- Jednoduché přičtení posunu d k ASCII kódu znaku (s kontrolou horní a spodní hranice rozsahu abecedy.
- Namapování vektorů abecedy OT a ŠT.

Monoalfabetické šifry: Reverzní abeceda (ATBASH)

šifra **ATBASH** [1]

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

- Nejstarší známá monoalfabetická šifra.
- Prostá reverze substitučních abeced
- Nemá klíč – klíčem je samotný princip (název)
- Algoritmizace většinou namapováním abeced nebo algebraricky.

Monoalfabetické šifry: Náhodná abeceda

26! možností (4.03×10^{26})

- Substituční abeceda je vytvořena jako jakákoliv náhodná permutace.
- Obrovský prostor možností abeced, což by z principu znemožnilo útok hrubou silou = zkoušení všech možností (permutací).
- Teoreticky zahrnuje i všechny zde uvedené příklady.
- Není klíč – klíčem je v podstatě znalost substituční abecedy [1].

Monoalfabetické šifry: Lineární posun

ax+*b* mod 26 neboli lineární posun

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

- Substituční abeceda je vytvořena jednoduchým vztahem.
- Klíčem jsou konstanty *a*,*b*.
- Při dešifrování je nutno dbát ohled na mod operaci – tedy dokud nezískám při zpětném šifrování celé kladné číslo, je nutné inkrementovat hodnotu znaku o 26 (někdy i opakovaně). Alternativně opět namapovat vektory abeced.
- Zde uvedený příklad $a = 3$, $b = 5$ (indexy znaků 0 – 25) [1].

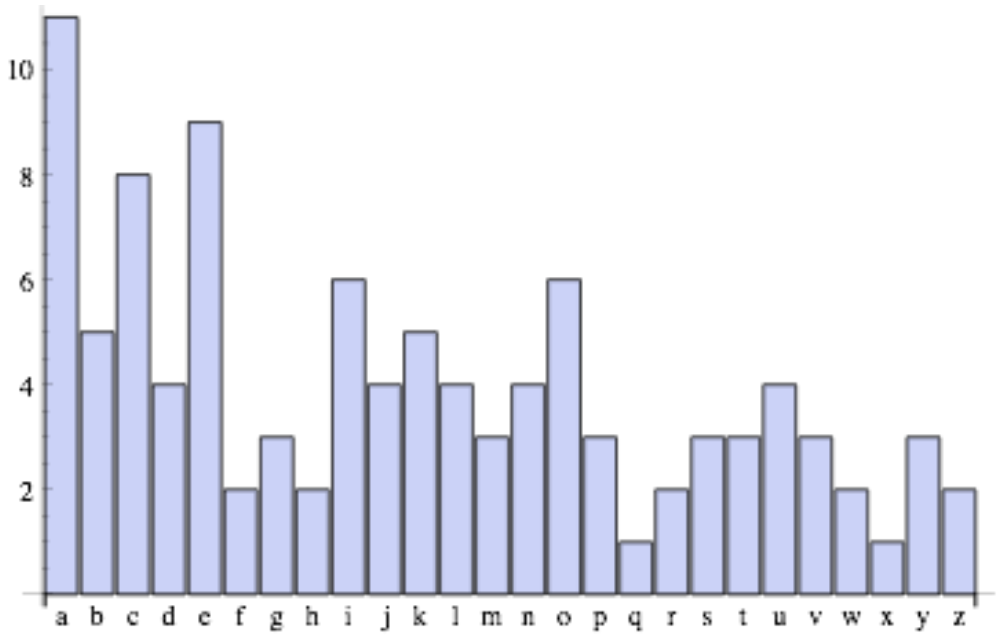
Monoalfabetické šifry: Substituce s klíčovým slovem

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

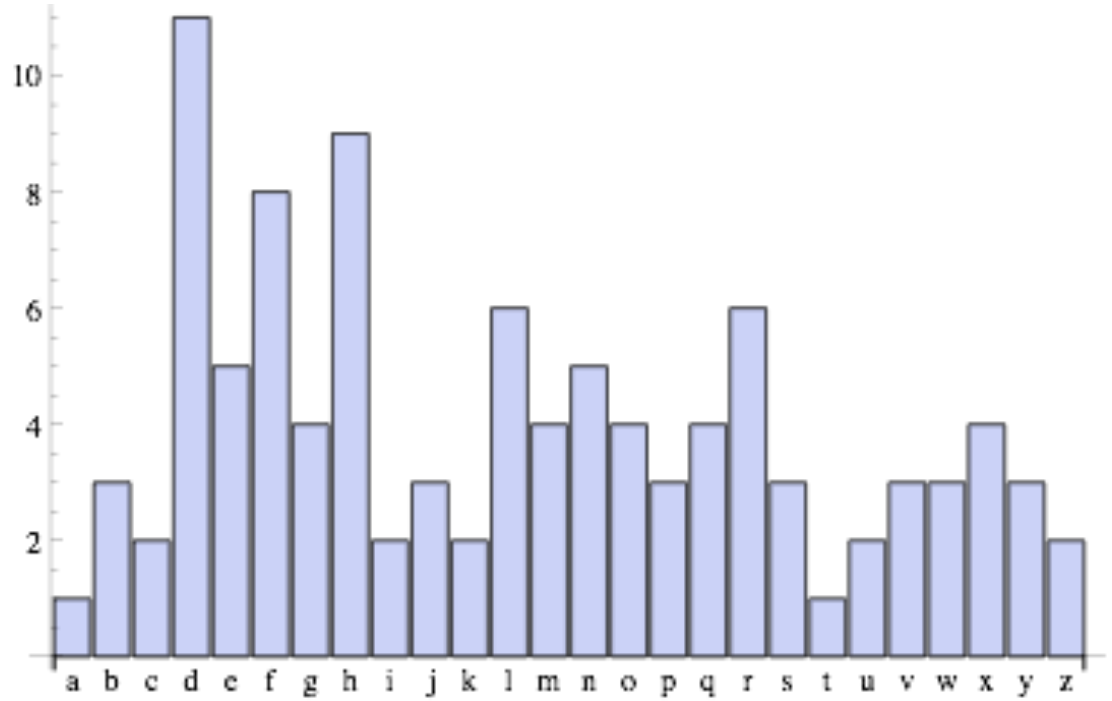
- Další jednoduchý systém.
- Nutno použít klíčové slovo, které obsahuje unikátní znaky (neopakující se).
- Klíčové slovo se napíše na začátek abecedy ŠT, dále se pokračuje výpisem abecedy s tím, že se přeskakují již použité znaky v klíčovém slově.
- Není jednoznačná algoritmizace, mimo namapování vektorů.
- Příklad dle [1].

Frekvenční analýza

Statistická analýza četnosti znaků.



OT

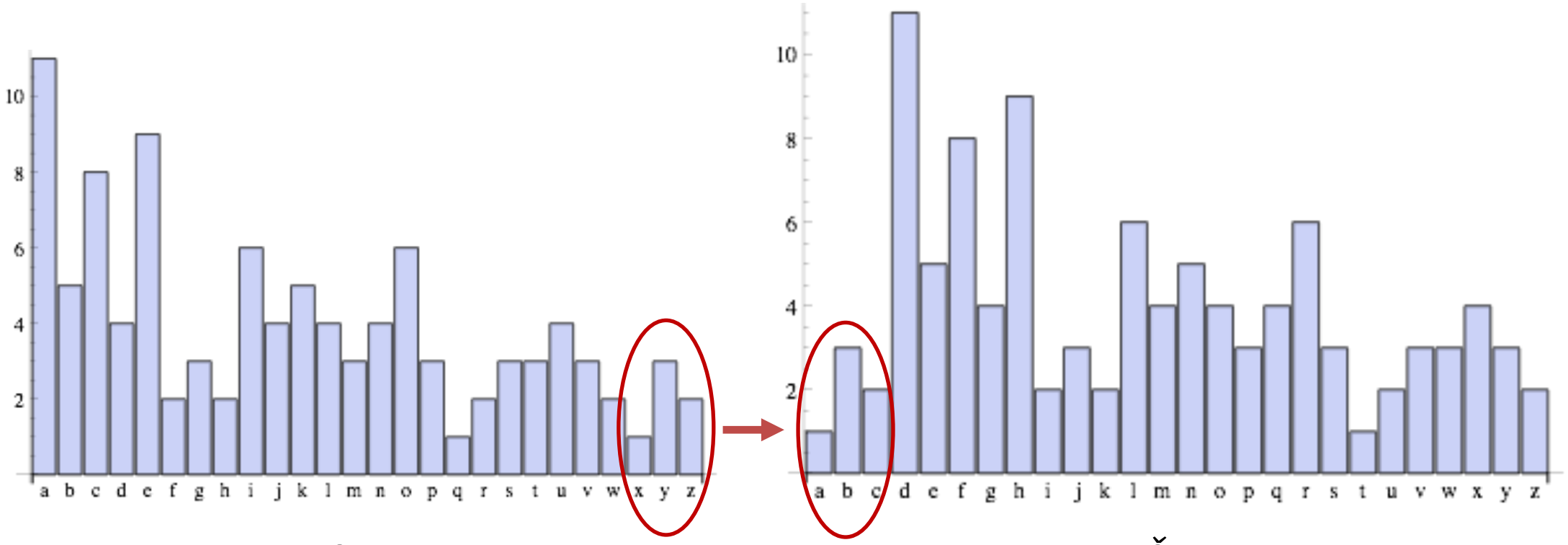


ŠT

Jaká byla použita šifra?

Frekvenční analýza

Statistická analýza četnosti znaků.



OT *ŠT*

CAESAROVA ŠIFRA – posun o 3 znaky „vpravo“

Frekvenční analýza

- Pomocí frekvenční analýzy lze rozhodnout zda se jedná o transpoziční či substituční systém.

- V případě substituce vede rychle k „prolinkování“ abeced. I když je prostor možností obrovský (viz náhodná abeceda – tedy 26! a útok hrubou silou je prakticky nemožný), díky přímé substituci statistických vlastností je luštění poměrně rychlé a efektivní.

- V případě transpoziční šifry odpovídá analýza OT přesně analýze ŠT – prosté „přeházení znaků nemá vliv na celkovou četnost.

2. Polyalfabetické šifry

Polyalfabetická šifra (Vigenérova)

- Založena na 26 monoalfabetických substitucích (v podstatě na 26 pevných posunech 0 - 25).
- Využívá klíčové slovo.
- Klíčové slovo řídí používání (střídání) jednotlivých substitucí.
- Pro šifrování i dešifrování je nutná tabulka Vigenerův čtverec tzv. “Tabulka Recta” [1].

Polyalfabetická šifra (Vigenérova): Princip

- Vzhledem k symetričnosti tabulky a jednoznačné relaci na monoalfabetickou šifru platí i jednoduchý vztah pro rychlou algoritmizaci:

$$ŠT = (OT + klíč) \bmod 26$$

- Dešifrování je pak jednoduchý proces:

$$OT = (ŠT - klíč) \bmod 26$$

Polyalfabetická šifra (Vigenérova): Princip

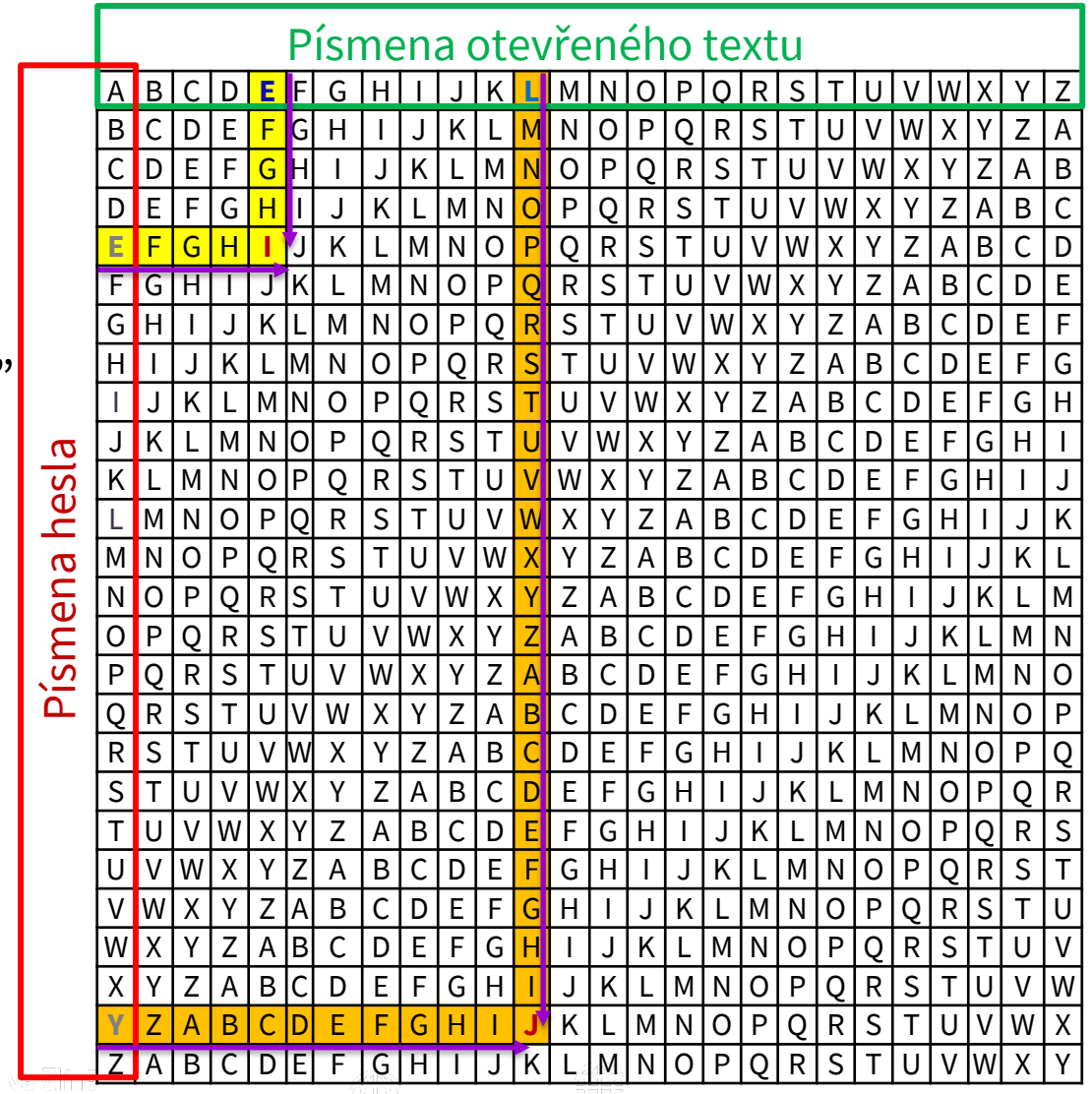
- Klíčové slovo se periodicky opakuje po celou délku OT.
- Hledáme průsečíky v Tabulce mezi znakem OT a znakem klíče (nebo použijeme jednoduchý vzorec).
- Frekvenční analýza není možná bez speciální a pracné celkové analýzy šifry. Musíme znát délku klíče a posléze provést náročnou n-násobnou frekvenční analýzu.

Polyalfabetické šifry - Vigenerova šifra: Příklad

Vigenerův čtverec (tabulka recta)

- Příklad
  - KEY = střídání tří “monoalfabetických substitucí”

OT:	H	E	L	L	O	T	I	M
Klíč:	K	E	Y	K	E	Y	K	E
ŠT:	R	I	J	V	S	R	S	O



3. Homofonní substituční šifry

Homofonní Substituce

- Homofonní substituce Je vylepšená monoalfabetická šifra, protože umožňuje šifrovat jedno písmeno z otevřené abecedy několika různými způsoby.

- Například písmeno „a“ může být v ŠT zastoupeno několika různými symboly, čímž luštiteli efektivně znemožníme použití jednoduché frekvenční analýzy.

Homofonní Substituce: Příklad

- Otevřený text: **LAKOMÁ LOKOMOTIVA**
- SUBSTITUČNÍ TABULKA:

A: 10 15 17	**K: 18**
O: 11 27 30	**M: 07 54**
I: 26	**T: 01**
L: 33 34	**V: 09**

- Šifruje se tak, že:
  - za A je na výběr 10, 15, 17 => zvolí se třeba 17
  - za L 33 nebo 34 => zvolí se třeba 33
  - a tak se postupuje až do konce.
- Šifrovaný text: **33 17 18 27 07 10 34 11 18 30 54 27 01 26 09 10**

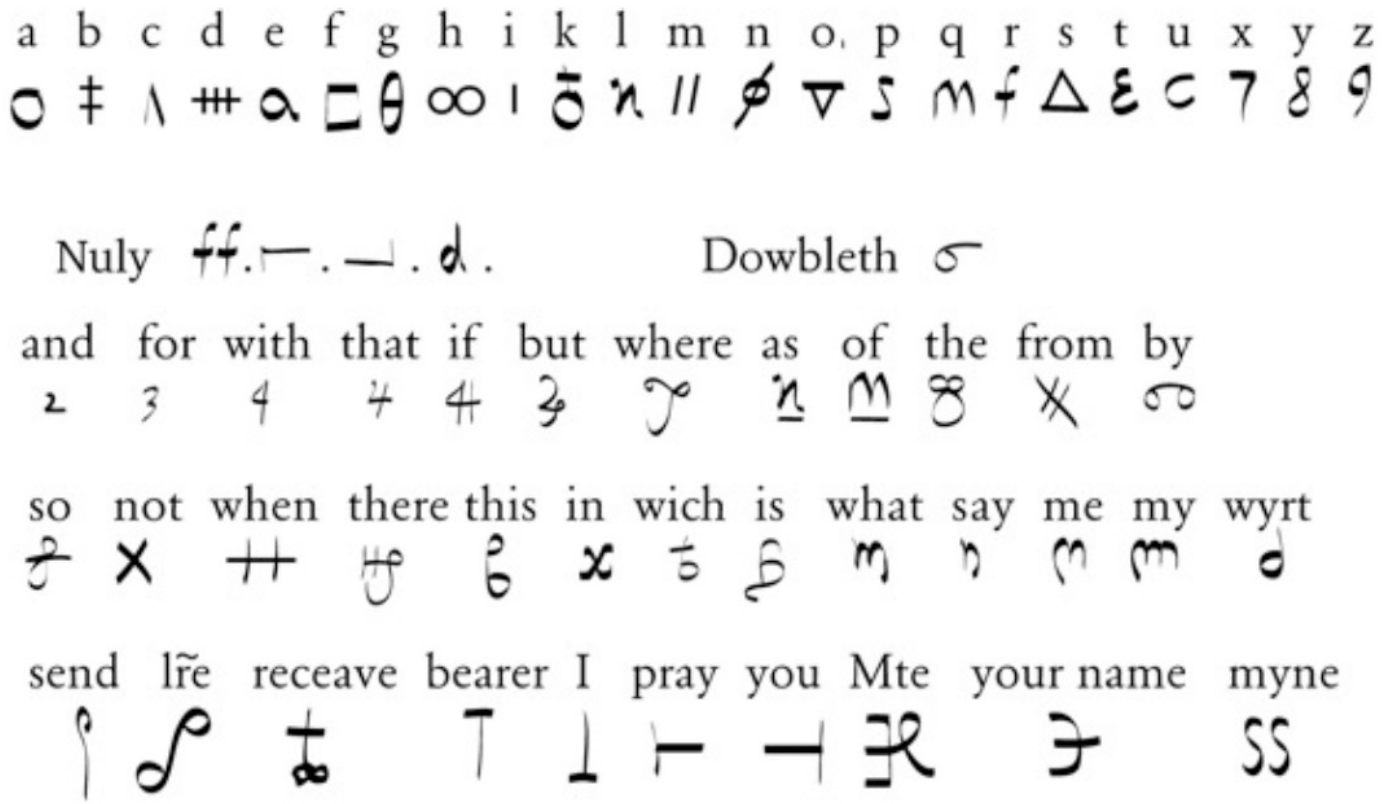
4. Další přístupy v substitučních šifrách

Ostatní Substituce - Nomenklátory a klamače

- Vybraným frekventovaným slovům se přiřadí speciální symbol. Tato kódová slova se nazývají nomenklátory [1].
- Klamač (nula) je dalším ztížení šifry, tyto znaky totiž nemají žádný význam, slouží pouze pro zmatení nepřítele [1].
- Další komplikace, která stíží analýzu je použití úmyslně zkomoleného textu [1].

Ostatní Substituce - Nomenklátory a klamače

Příkladem může být šifra **Marie Stuartovny** [2]:



Seznam odkazů

[1] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Praha: Portál, 2007. ISBN 978-80-7367-196-9.

[2] SINGH, Simon. Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii. 2. vyd. v českém jazyce. Přeložil Dita ECKHARDTOVÁ, přeložil Petr KOUBSKÝ. Praha: Dokořán, 2009. Aliter (Argo: Dokořán). ISBN 978-80-7363-268-7.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204