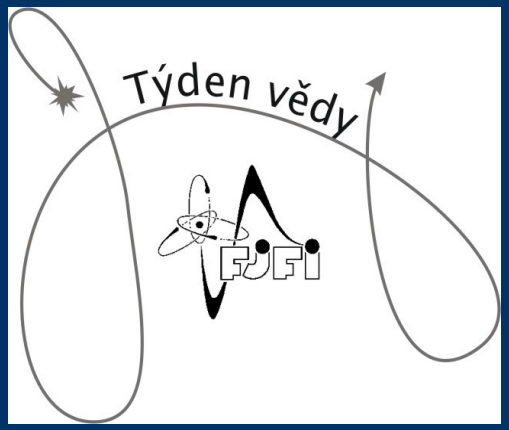


Šifrování

10110011000111011100011101010111011011101010010010111011101010001011
10101001011010010101011101010101011010101010100101010101011101010101

[1]Ondřej Maslikiewicz, [2]Ondřej Hujňák, [3]Jiří Stejskal

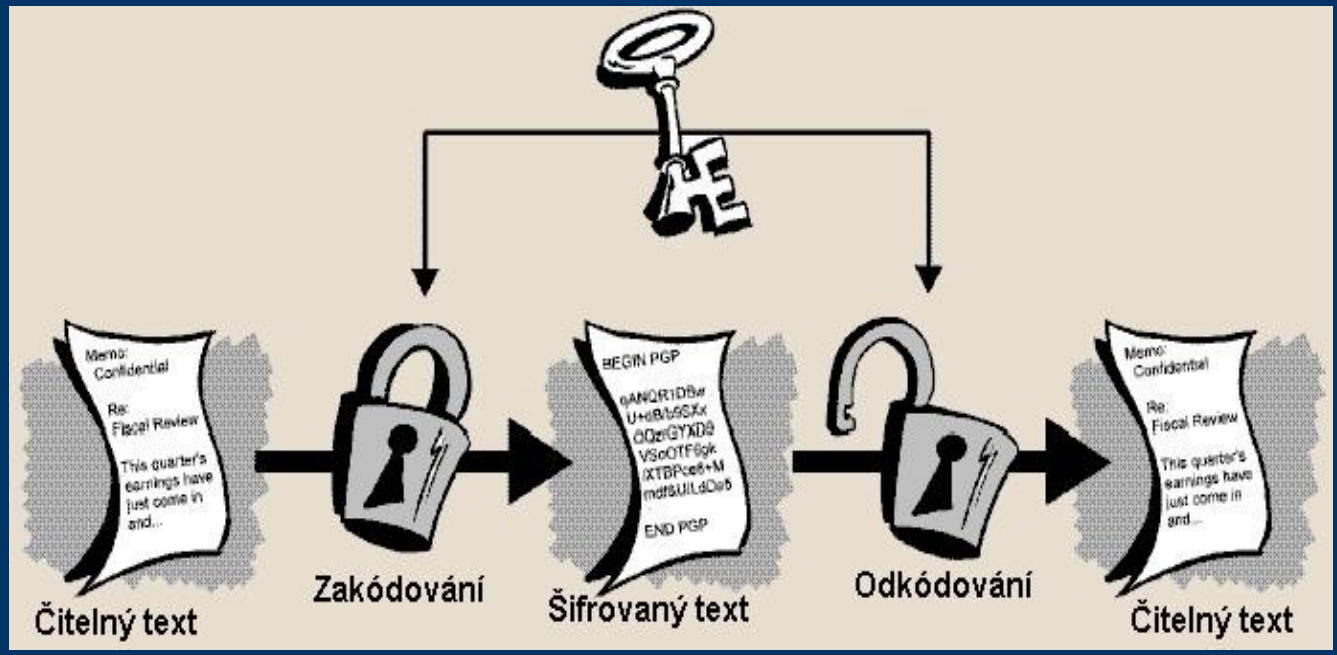
[1]Střední průmyslová škola Hronov
[2]Gymnázium Slovanské nám.
[3]Gymnazium Děčín

Co vás čeká (a nemine)

- Význam a historie šifrování
- Rozdělení šifer
- Příklady nejznámějších šifer
- Šifrovací program

K čemu nám šifrování je?

- Email
- Internet
- Banky
- Politika
- Válka
- Elektronika



Historie šifrování

- Více než 2000 let
- Válečné konflikty

Rozdělení šifer

- Symetrické
- Asymetrické

- Substituční
- Transpoziční

Symetrické šifry

Caesarova šifra

- Posun písmen abecedy
- Klíč celé číslo
- 26 možných klíčů při anglické abecedě
- Náchylná na prolomení

Afinní šifra

- Podobná předcházející
- Má dva parametry

  $Ci = (a*Ti + b) \bmod m$

- **Mod m** je zbytek po celočíselném dělení

Polybiův čtverec

- Základem je čtverec 5x5
- I a J mají jedno políčko
- Znaky se nahrazují souřadnicemi
- Př: a = 11, f = 21

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

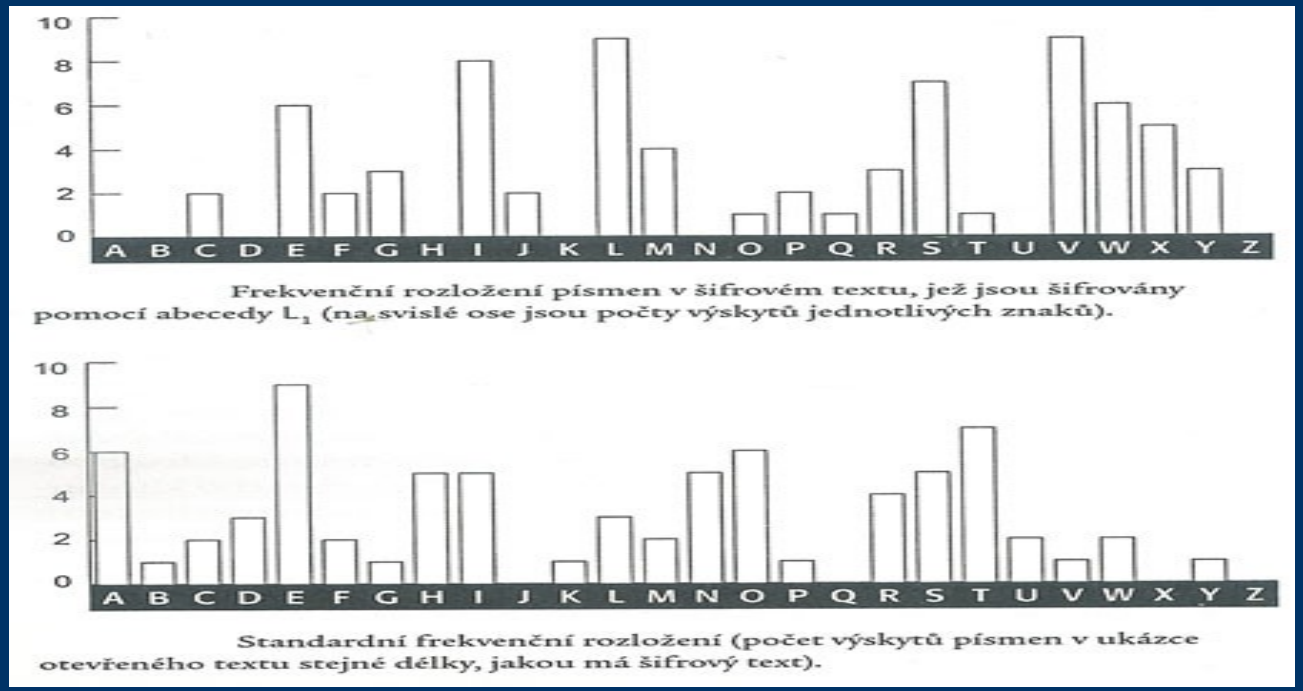
Playfairova šifra

- Základ opět ve čtverci
- Abeceda nejde popořadě, začíná se klíčem, kde se vynechají stejná písmena a doplní se zbytek abecedy
- Šifruje se bigram
- Podle pravidel:

-nachází-li se v řádku, posuneme je o jedno doprava
-nachází-li se ve sloupci, posuneme je o jedno dolů
-posuneme první písmeno bigramu dolů až na řádek, na kterém se nachází druhé písmeno a druhé písmeno posuneme analogicky nahoru.

Homofonní šifra

- Na rozdíl od předešlých šifer je odolná proti frekvenční analýze
- Znáhodňující prvky
- Stejný znak z otevřeného textu má více přiřazovaných znaků



Frekvenční rozložení písmen v šifrovém textu, jež jsou šifrovány pomocí abecedy L_1 (na svislé ose jsou počty výskytů jednotlivých znaků).

Standardní frekvenční rozložení (počet výskytů písmen v ukázce otevřeného textu stejné délky, jakou má šifrový text).

Polyalfabetická šifra

- Vyhlazuje frekvence v histogramu
- Jeden znak šifrovaného resp. otevřeného textu neodpovídá vždy jednomu znaku v otevřeném resp. šifrovaném textu.
- Vinegerova šifra – nejznámější
  (3 stol. Neprolomena)

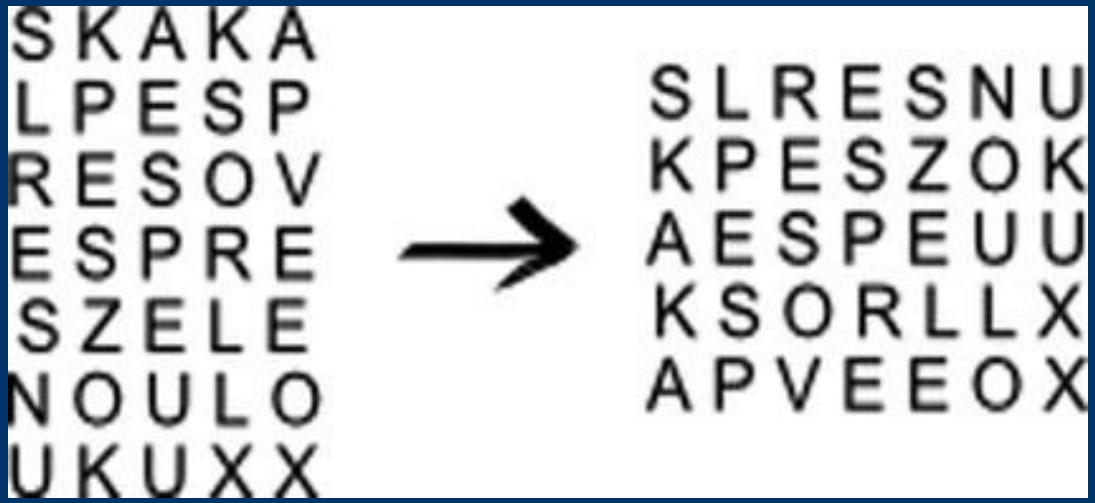
Vinegèrova šifra

- Otevřený text: P L A I N T E X T
- Klíč: S L I Z O U N S L

	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

Transpoziční šifra

- Zamění se pořadí znaků v otevřeném textu
- Klíč je malé celé číslo
- Dešifrovací klíč = Počet písmen textu / šifrovací klíč



Superšifrování

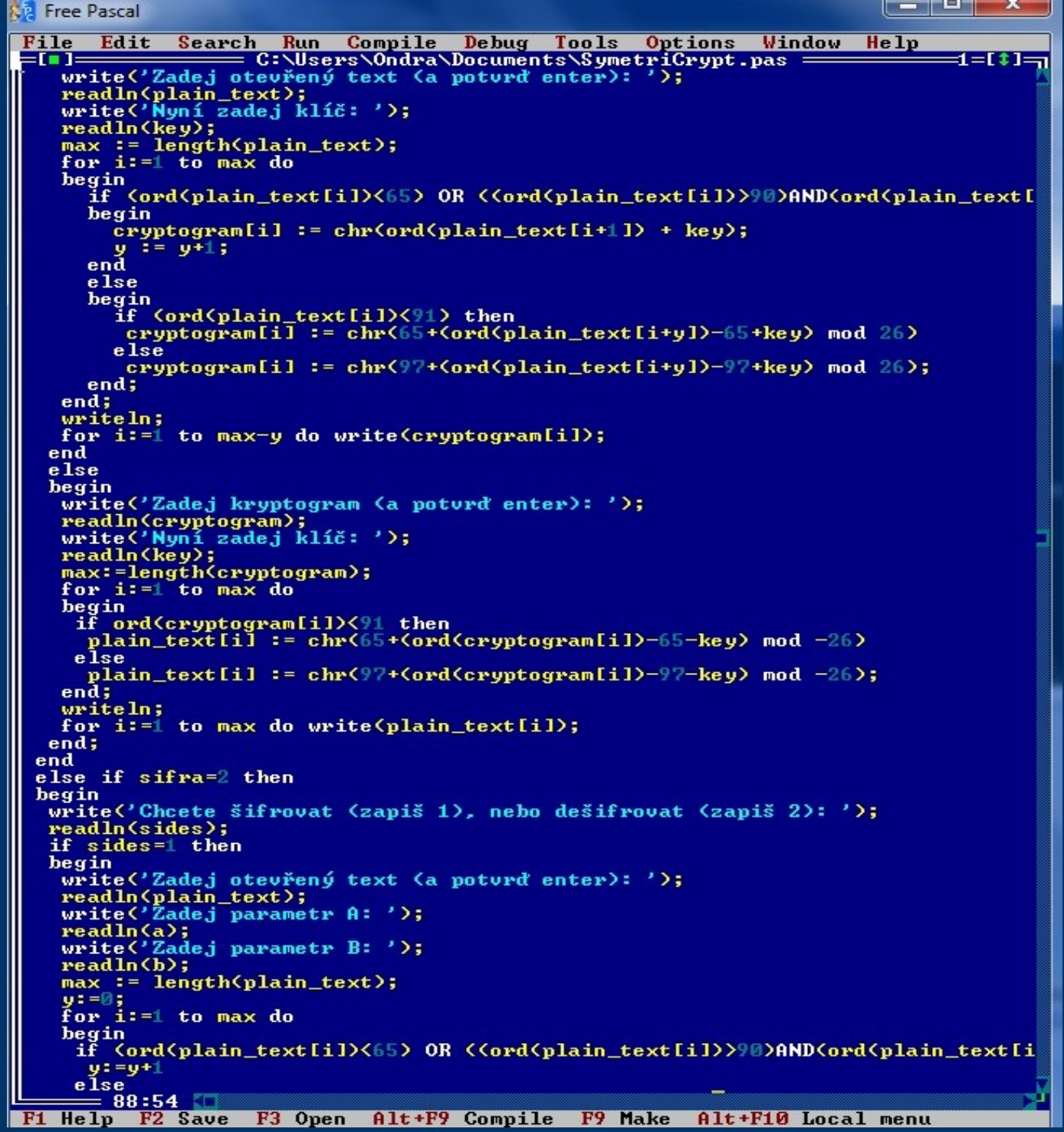
- Použití více různých šifer (algoritmů) za sebou
- Minimalizace rizika prolomení
- Zpomalení dešifrování

Program

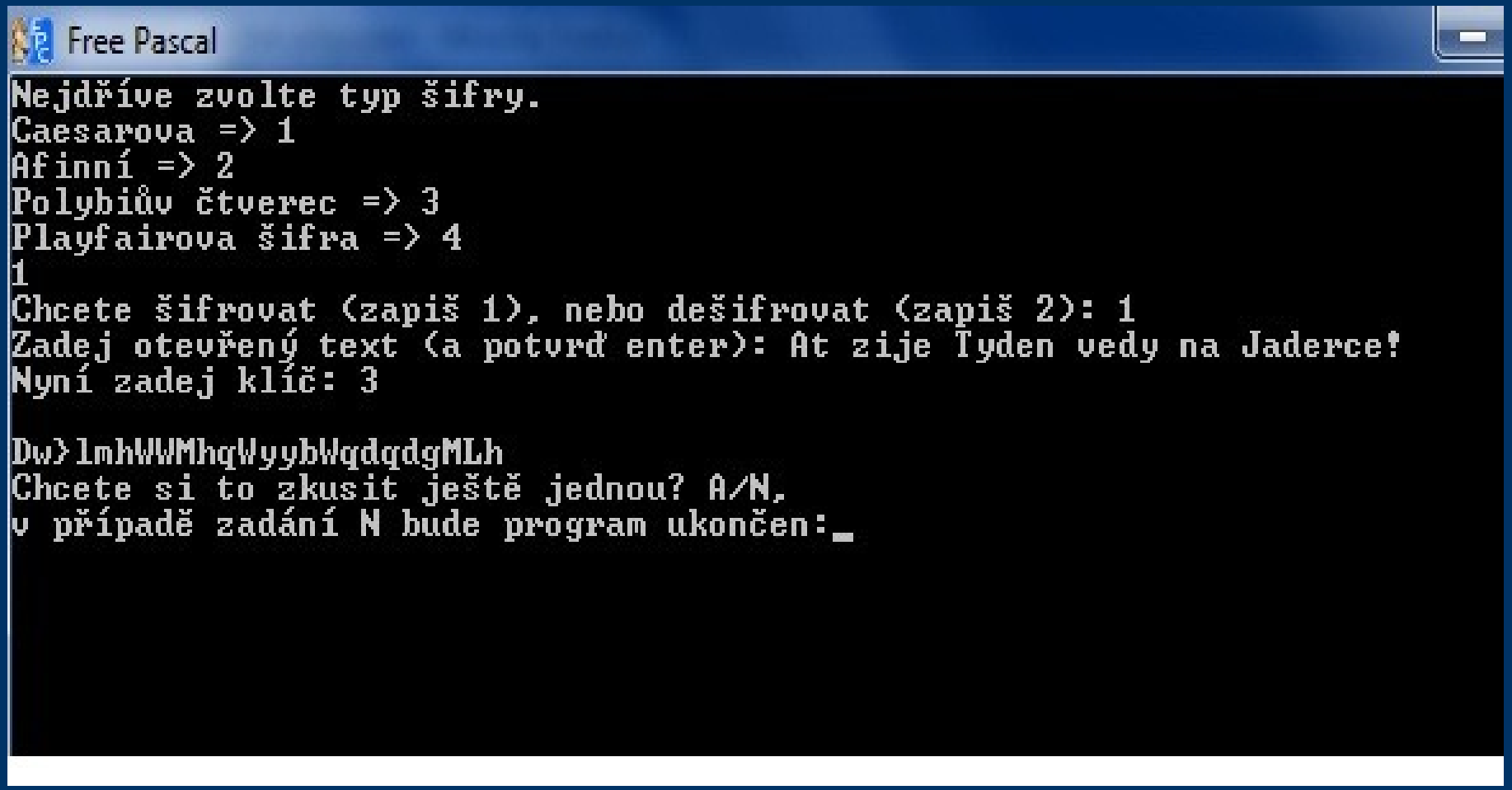
- V programovacím jazyce Pascal

- Caesarova šifra
- Odolný vůči mezerám a speciálním znakům

- Afinní šifra

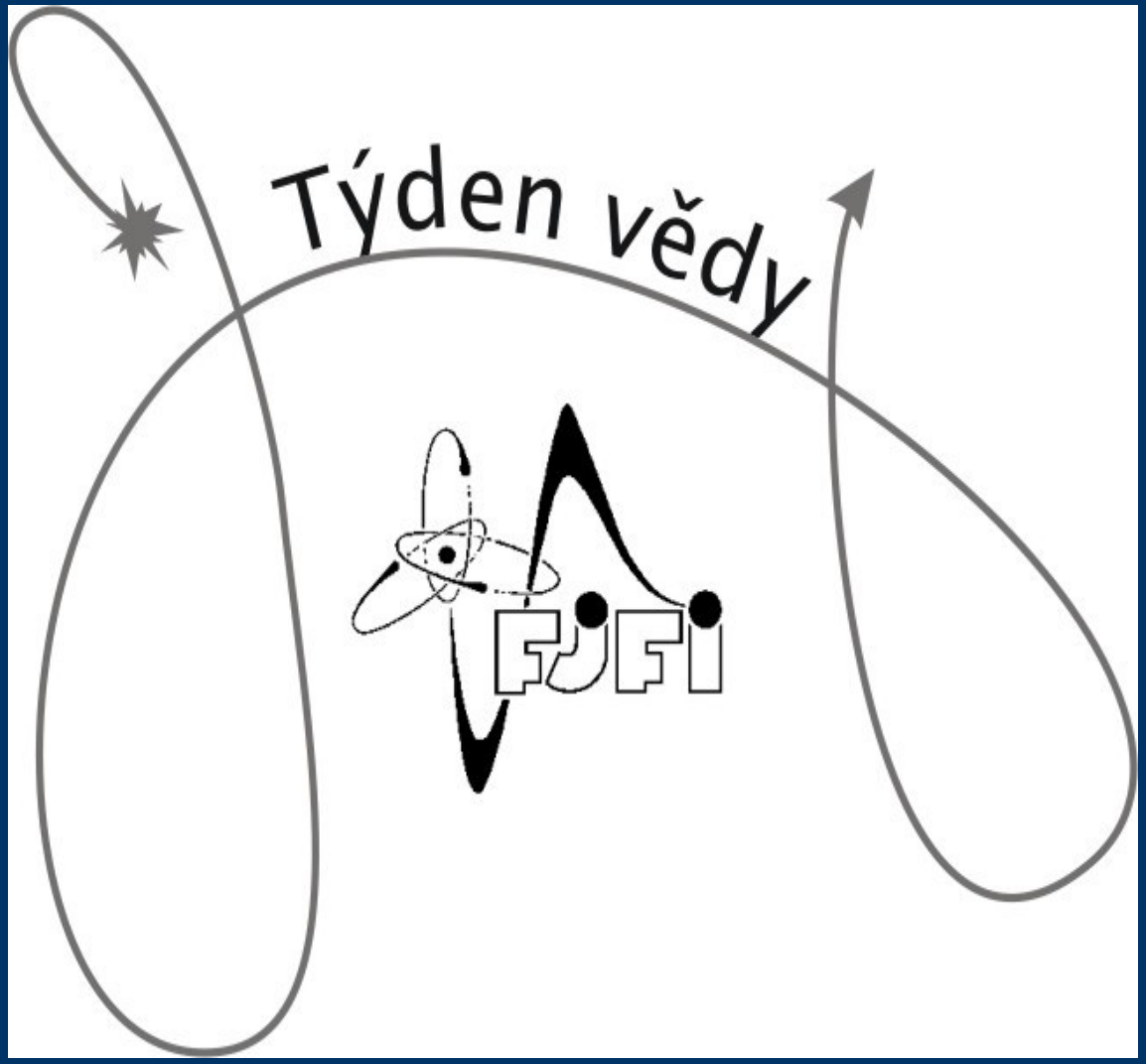

Free Pascal
File Edit Search Run Compile Debug Tools Options Window Help
C:\Users\Ondra\Documents\SymetriCrypt.pas
write('Zadej otevřený text (a potvrď enter): ');
readln(plain_text);
write('Nyní zadej klíč: ');
readln(key);
max := length(plain_text);
for i:=1 to max do
begin
if (ord(plain_text[i])<65) OR ((ord(plain_text[i])>90)AND(ord(plain_text[
begin
cryptogram[i] := chr(ord(plain_text[i+1]) + key);
y := y+1;
end
else
begin
if (ord(plain_text[i])<91) then
cryptogram[i] := chr(65+(ord(plain_text[i+y])-65+key) mod 26)
else
cryptogram[i] := chr(97+(ord(plain_text[i+y])-97+key) mod 26);
end;
end;
writeln;
for i:=1 to max-y do write(cryptogram[i]);
end
else
begin
write('Zadej kryptogram (a potvrď enter): ');
readln(cryptogram);
write('Nyní zadej klíč: ');
readln(key);
max:=length(cryptogram);
for i:=1 to max do
begin
if ord(cryptogram[i])<91 then
plain_text[i] := chr(65+(ord(cryptogram[i])-65-key) mod -26)
else
plain_text[i] := chr(97+(ord(cryptogram[i])-97-key) mod -26);
end;
writeln;
for i:=1 to max do write(plain_text[i]);
end;
end
else if sifra=2 then
begin
write('Chcete šifrovat (zapiš 1), nebo dešifrovat (zapiš 2): ');
readln(sides);
if sides=1 then
begin
write('Zadej otevřený text (a potvrď enter): ');
readln(plain_text);
write('Zadej parametr A: ');
readln(a);
write('Zadej parametr B: ');
readln(b);
max := length(plain_text);
y:=0;
for i:=1 to max do
begin
if (ord(plain_text[i])<65) OR ((ord(plain_text[i])>90)AND(ord(plain_text[i
y:=y+1
else
88:54
F1 Help F2 Save F3 Open Alt+F9 Compile F9 Make Alt+F10 Local menu

Takhle to funguje!



Zdroje

- Kryprografie, F. Piper, S. Murphy, nakladatelství Dokořán, 2006
- Rozluštěná tajemství, J. Janeček, nakladatelství XYZ, vydání druhé, 2008
- www.security-portal.cz



Děkujeme za pozornost.