

OBSAH

ÚVOD	5
1. ZÁKLADY ANALÝZY ŠIFER	7
1.1. Základní definice	7
1.2. Statistické charakteristiky otevřeného a šifrovaného textu	8
1.2.1. Četnosti	8
1.2.2. Součet čtverců pravděpodobností	9
1.2.3. <i>n</i> -místná opakování písmen (znaků)	10
1.2.4. Shody mezi telegramy	11
1.2.5. Počet chybějících písmen v textu	11
1.2.6. Charakteristika polohy znaku	12
1.2.7. Test jednoabecednosti	12
1.2.8. Test periodičnosti	15
1.2.9. Redukovaný test jednoabecednosti	16
1.3. Charakteristika některých jazyků	17
1.3.1. Četnosti <i>n</i> -místných opakování	17
1.3.2. Často používaná slova (stereotypy)	17
1.3.3. Neobvyklá slova	17
1.3.4. Postavení samohlásek a souhlásek ve slovech	17
1.3.5. Charakteristiky českého jazyka	17
1.3.5.1. Četnosti písmen (v %):	18
1.3.5.2. Opakování bigramů a trigramů	18
1.3.6. Charakteristiky anglického jazyka	19
1.3.6.1. Četnosti písmen (v %):	19
1.3.6.2. Opakování bigramů a trigramů	19
1.3.7. Charakteristiky francouzského jazyka	20
1.3.7.1. Četnosti písmen (v %):	20
1.3.7.2. Opakování bigramů a trigramů	20
1.3.8. Charakteristiky německého jazyka	21
1.3.8.1. Četnosti písmen (v %):	21

1.3.8.2. Opakování bigramů, trigramů a tetragramů.	21
1.3.9. Charakteristiky španělského jazyka	22
1.3.9.1. Četnosti písmen (v %):	22
1.3.9.2. Opakování bigramů a trigramů.	22
1.3.10. Charakteristiky italského jazyka	23
1.3.10.1. Četnosti písmen (v %):	23
1.3.10.2. Opakování bigramů a trigramů	23
2. TRANSPOZIČNÍ SYSTÉM	25
2.1. Jednoduchá transpozice	25
2.2. Metoda plukovníka Roche	26
2.3. Jednoduchá transpozice v tabulce	27
2.4. Mřížka	27
2.5. Zubatka	30
2.6. Jednoduchá transpozice v tabulce se dvěma hesly	32
2.7. Dvojitá transpozice	33
2.8. Dvojitá transpozice s upravenou tabulkou 1 a doplněnou tabulkou 2	34
2.9. Luštění jednoduché transpozice v tabulce	36
2.10. Luštění mřížky	48
2.11. Luštění dvojitě transpozice	55
2.12. Luštění dvojitě transpozice s upravenou tabulkou 1 a doplňovanou tabulkou 2	62
Cvičení ke kapitole 2	69
3. SUBSTITUČNÍ SYSTÉM	73
3.1. Jednoduchá záměna	74
3.2. Více šifer za písmeno	75
3.3. Složitá záměna	77
3.4. Autokláv	81
3.5. Složitá substituce s rozházenou abecedou	82
3.6. PLAYFAIR neboli anglický čtverec	83

3.7. Jednotkové připočítání hesla	85
3.8. Luštění jednoduché záměny	87
3.9. Luštění více šifer za písmeno	92
3.10. Luštění složité záměny	95
3.11. Luštění autoklávu - OT	102
3.11.1. Využití chyby pro luštění autoklávu-OT	102
3.11.2. Luštění autoklávu-OT z více telegramů zašifrovaných stejným základním heslem	105
3.12. Luštění autoklávu-OT z jediného telegramu	107
3.13. Luštění složité substituce s rozházenou abecedou	110
3.14. Luštění anglických čtverců	117
3.15. Luštění šifer s jednotkově připočítaným heslem	119
Cvičení ke kapitole 3	122
4. ŠIFROVACÍ TABULKY A KÓDY	129
4.1. Šifrovací tabulky	129
4.2. Kódy	131
4.3. Kniha jako kód	132
4.4. Luštění šifrovacích tabulek a kódů	132
Souhrnná cvičení pro 2. a 3. kapitolu	141
ZÁVĚR	145
Některé výsledky cvičení z kapitol 2 a 3	145
PROGRAMOVÉ VYBAVENÍ	147
Tisk tabulek opakování písmen v náhodném textu	147
Tisk tabulek opakování číslic v náhodném textu	149
Podprogram pro tisk na tiskárně EPSON	151
Program pro nalezení opakování	153
Podprogram pro rychlé vyhledávání opakování	154

Program pro výpočet koeficientu K při rozpisu písmenkového tlg pro periody 2 až 50	156
Podprogram pro rychlý výpočet K	158
Program pro výpočet koeficientu K při rozpisu číslíkového tlg pro periody 2 až 50	162
Program pro sunutí slov otevřeného textu v telegramu zašifrovaném autoklávem OT	163
PŘÍLOHY	167
Příloha 1/1 Tabulka četností bigramů pro český jazyk	168
Příloha 1/2 Četnosti písmen českého a slovenského jazyka bez mezer mezi slovy (mezinárodní abeceda) a četnosti českého jazyka se znaménky	169
Příloha 1/3 Četnosti písmen (v %) několika evropských jazyků	170
Příloha 1/4 Tabulka četností bigramů pro český jazyk	171
Příloha 3.8/1 Trigramový arch	172
Příloha 3.8/2 Trigramový arch	173
Příloha 3.15/1 Formulář pro tabulku četností číselných bigramů	174
Příloha 4.1/1 Vojenská hovorová tabulka typu "SLIDEX"	175
Příloha 4.1/2 Vojenská šifrovací tabulka	176