Univerzita Hradec Králové
Přírodovědecká fakulta
Katedra Kybernetiky

Počítačová analýza šifrované korespondence rodu Piccolomini

Bakalářská práce

Autor: Václav Vlnas
Studijní program: B1801 Informatika
Studijní obor: Informatika se zaměřením na vzdělávání
Historie se zaměřením na vzdělávání
Vedoucí práce: PhDr. Michal Musílek, Ph.D.

Hradec Králové 2017

Univerzita Hradec Králové
Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	**Václav Vlnas**
Studium:	S13173
Studijní program:	B1801 Informatika
Studijní obor:	Informatika se zaměřením na vzdělávání
Název bakalářské práce:	**Počítačová analýza šifrované korespondence rodu Piccolomini**
Název bakalářské práce AJ:	Computer Analysis of Encrypted Correspondence of House of Piccolomini

Cíl, metody, literatura, předpoklady:

Práce se bude zabývat počítačem podporovanou analýzou šifer adresovaných většinou Ottaviovi Piccolomini, nebo jím psaných, koncem 16. a začátkem 17. století. Použité typy šifer budou zasazeny do kontextu historického vývoje kryptologie. Autor práce připraví skripty v jazyce Visual Basic for Applications ve vývojovém prostředí tabulkového procesoru Microsoft Excel, které poslouží k frekvenční analýze a postupnému prolomení šifrovacího klíče (substituční tabulky) jednotlivých šifer a následnému dešifrování. Úkol je objektivně ztížen skutečností, že otevřené texty šifer pravděpodobně nebudou v českém jazyce, nýbrž v italštině, francouzštině či latině. Praktickým výstupem práce budou skripty v jazyce Visual Basic for Applications, fotokopie historických šifrových dokumentů a jejich dešifrovaná podoba (otevřený text vybraných dokumentů).

Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.
Oponent:	doc. RNDr. Štěpán Hubálovský, Ph.D.

Datum zadání závěrečné práce: 7.10.2016

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně pod vedením PhDr. Michala Musílka, Ph.D. a že jsem v seznamu literatury uvedl všechny použité prameny a literaturu.

V Hradci Králové dne

.....

Jméno a příjmení

Poděkování

Rád bych poděkoval PhDr. Michalu Musílkovi, Ph.D., za velký zájem, za vedení, cenné rady a čas, kterým přispěl k vypracování této bakalářské práce. Dále bych chtěl poděkovat pracovníkům SOA Zámrsk za vřelé jednání a pomoc při hledání. V neposlední řadě bych chtěl poděkovat též mým kamarádům a rodině za pomoc a podporu.

Anotace

VLNAS, Václav. *Počítačová analýza šifrované korespondence rodu Piccolomini.* Hradec Králové: Přírodovědecká fakulta Univerzity Hradec Králové, 2017. 72 s. Bakalářská práce.

Tématem bakalářské práce bylo podrobit zašifrované historické texty analýze a pokusit se dešifrovat tyto dokumenty. K tomuto cíli byla využita podpora maker programovacího jazyka VBA v programu Microsoft Excel. Výsledná práce se skládá ze čtyř kapitol. V první z nich je popsán vývoj kryptografie a nastíněna problematika šifer jak konkrétních, tak i obecných. Druhá kapitola je věnována MS Excel a jeho využití k dešifrování a analýze šifer. Ve třetí kapitole je zachycen vzestup rodu Piccolominiů a život jednoho jejich člena, Otavia Piccolomini. Poslední čtvrtá kapitola je věnována samotným šifrám. V této kapitole je obsažen přepis šifer i s mezířádkovým dešifrováním. Všechny postupy a klíčové body kryptoanalýzy jednotlivých šifer jsou patřičně okomentovány a vysvětleny.

Klíčová slova: šifry, kryptologie, kryptografie, Piccolomini, Excel, VBA, makra

Annotation

VLNAS, Václav. *Computer Analysis of Encrypted Correspondence of House of Piccolomini.* Hradec Králové: Faculty of Natural Science, University of Hradec Králové, 2017. 72 p. Bachelor Thesis.

The topic of this bachelor thesis was to subject the encrypted historical texts to analysis and to try to decrypt these documents. To this end, for support was used VBA macros in programming language in Microsoft Excel. The final work consists of four chapters. In the first one the development of cryptography is described and the problems of ciphers of particular and general ones are outlined. The second chapter is dedicated to MS Excel and its use for decryption and cipher analysis. In the third chapter, the rise of the Piccolomini family and the life of one of their members, Otavio Piccolomini, is captured. The last fourth chapter is dedicated to the ciphers themselves. This chapter includes both the cipher and the inter-line decryption. All procedures and key points of cryptanalysis of each cipher are properly commented and explained.

Keywords: ciphers, cryptology, cryptography, Piccolomini, Excel, VBA, macros

Obsah

Úvod

Tato bakalářská práce se zabývá historickými šiframi, adresovanými Otaviovi Piccolomini, a jejich kryptoanalýze prostřednictvím tabulkového procesoru Microsoft Excel. Cílem této práce je podrobit archivní šifrové texty analýze a na základě této analýzy se pokusit šifry rozluštit buď úplně, nebo alespoň částečně. Účinnou pomocí je využití maker vytvořených v programovacím jazyce Visual Basic for Applications (dále jen VBA), který je obsažen v tabulkovém procesoru MS Excel. Makra umožní provést frekvenční analýzu, díky které lze částečně doplnit dešifrovací tabulky a vytvořit frekvenční spektrum, z jehož složení lze s velkou mírou pravděpodobnosti určit jazyk, jakým byl dokument napsán. Další makra umožní po doplnění dešifrovací tabulky metodou předpokládaných slov provést automatické dešifrování do otevřeného textu, čímž odpadne rutinní a monotónní práce ve srovnání s klasickým ručním dešifrováním.

Práce je členěna do několika kapitol a podkapitol. V první kapitole s názvem Kryptologie je v úvodním odstavci popsáno, co je vlastně kryptologie a jaké jsou její základní pilíře. Tato kapitola je rozdělena do čtyř podkapitol. V první z nich je popsán historický vývoj kryptografie, kde je tento vývoj doplněn ilustracemi a doplňujícími tabulkami pro lepší pochopení některých druhů šifer, které v minulosti vznikly. V další podkapitole je popsáno, co to je vlastně kryptografie. Je zde vysvětleno rozdělení šifer, jejich použití, různé metody komplikací šifer apod. V podkapitole Kryptoanalýza je vysvětleno proč vznikla, jaké jsou její cíle, a jaké používá metody. V poslední z podkapitol, nazvané Steganografie, je stručně popsáno, čím se tato nauka zabývá a jsou zde uvedeny i příklady využití.

Druhá kapitola s názvem Microsoft Excel se zabývá stručným vývojem tohoto programu, dále se též zabývá popisem vybraných syntaktických konstrukcí programovacího jazyka VBA, jejichž prostřednictvím je uživatel schopný psát v MS Excel makra.

Třetí kapitola je věnována rodu Piccolominiů, z jehož rodového archivu byly vybrány historické šifry ke kryptoanalýze. V této kapitole je charakterizováno, jak a proč se tento rod dostal na výsluní a díky čemu tím dosáhli úspěchů. V závěru kapitoly jsou zmíněni nejslavnější členové rodu. Tato kapitola má dvě podkapitoly. V první z nich je stručný životopis Otavia Piccolominiho, jehož šifry byly použity jako základ této práce. Je zde také podkapitola, která je věnována mé návštěvě Státního oblastního

archivu (dále jen SOA) Zámrsk, kde jsem stručně popsal celou návštěvu tohoto archivu i s orientací v systematice zdejších dokumentů z důvodu snazšího nalezení konkrétních listin.

Následuje poslední, čtvrtá, kapitola. Cílem této kapitoly je se pokusit, alespoň částečně, dešifrovat zašifrované texty. Tato kapitola nese název Zašifrované dokumenty. Tento název však zastřešuje několik šifer, které jsou samostatně rozebrány ve čtyřech podkapitolách. V každé podkapitole se jako první vyskytuje název dokumentu (pojmenováno inventárními čísly z archivu). Následně je zde dešifrovací tabulka, někdy v podobě šifrového čtverce, někdy jako dvouřádková substituční tabulka, ke které je vždy napsán komentář, ve kterém je zachyceno mnoho specifických poznatků. Například to jakým šifrovacím systémem je šifra psána, nebo z jakého známého systému vychází, dále pak konkrétní zvláštnosti dané šifry apod. Za popisem je vždy publikována samotná šifra a její mezířádkový dešifrovaný přepis, který byl vytvořen makrem ve VBA. Tyto podkapitoly obsahují kódy použitých maker, které jsou rozebrány a okomentovány a je vysvětlen jejich princip a účel. Dále podkapitoly obsahují tabulky četnosti znaků získané počítačovou frekvenční analýzou textů a k tomu příslušné grafy pro lepší názornost a přehlednost.

1 Kryptologie

Kryptologie je věda, která se zabývá texty, u kterých je zpravidla část, nebo celý text utajen. Někdy se pojem kryptologie používá se spojení se vším, kde objevují šifry. Tato věda je rozdělena do několika dalších vědních oborů, které jsou její páteří a bez kterých by tato věda nemohla existovat. Jsou jimi kryptografie – zabývající se vývojem šifer, dále kryptoanalýza, bez které by je nebylo možno rozluštit, a nakonec steganografie, která tají samotnou existenci zpráv. (Vondruška, 2006, s. 8), (Janeček, 2006, s. 14–15)

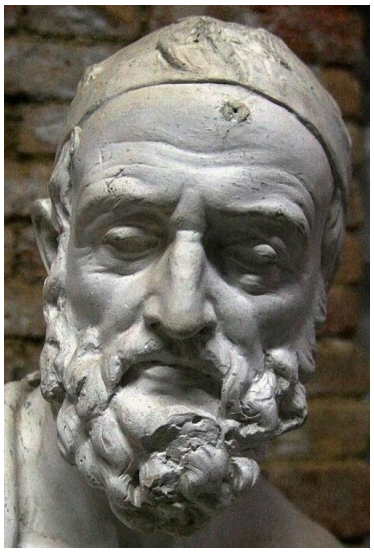
1.1 Historie kryptografie

Historie kryptografie je velmi dlouhá, první zmínky se datují kolem roku 1900 př. n. l. v Egyptě, kde byly nalezeny v jedné hrobce hieroglyfy, které se lišili od ostatních. Jejich funkce byla upoutat svojí zvláštností. Staré šifry nebyly pouze ve starém Egyptě, ale můžeme je též nalézt ve staré Mezopotámii, kde se našla destička s klínovým písmem. Tato destička se datovala okolo roku 1500 př. n. l. a lišila se od ostatních tím, že na ní byla objevena šifra, která skrývala profesní tajemství na výrobu glazované keramiky. Na této destičce bylo využito jednoduché záměny znaků klínové abecedy. Na předním východě se objevila ještě jedna známá šifra a tou byla Atbaš, kterou vymysleli Hebrejci v 5. století př. n. l. Tato šifra využívala jednoduchou substituci. V praxi to fungovalo tak, že se vzalo pořadí písmene od začátku a vyměnilo se písmenem se stejným pořadím od konce abecedy. Hebrejci používali ještě dvě šifry a to atbam a albam. (Vondruška, 2006, s. 196–197)

Velmi zásadním posunem v kryptografii bylo zapojení řecké kultury. V 5. a 6. století př. n. l. se objevuje ve starověké Spartě šifra se jménem Skytala, nebo také Scytala, která fungovala na mechanickém způsobu zašifrování. Toto jméno dostala od hole, která měla přesný poloměr, který byl nezbytný k rozluštění šifry. Odesílatel musel použít proužek kůže, který omotal kolem skytaly, následně napříč napsal obsah zprávy. Poté, co pásek sundal, nedávala zpráva smysl. Tato šifra však byla omezena tak, že příjemce i odesílatel museli mít stejný průměr hole, jinak nebylo možné zprávu přečíst. (Singh, 1999, s. 8–9)

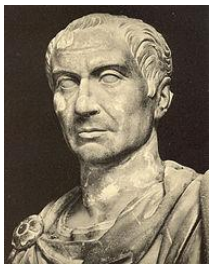
Obrázek č. 1 – Skytala

V Řecku se využívala jednoduchá záměna samohlásek za tečky, později se písmena nahrazovala číslicemi. V řecké kultuře můžeme najít ve 2. století př. n. l. ještě jeden typ šifry, který vymyslel řecký spisovatel Polybios a po kterém je také pojmenována. Tato šifra připomíná šachovnici, protože je tvořena číslicemi, které jsou nadepsány svisle i vodorovně. Spojením těchto dvou číslic dostaneme písmeno nebo znak. Tento tzv. Polybiův čtverec byl hojně využíván i v pozdější době, například rod Piccolominiů využívá hojně tento systém šifrování, ač je upravený a využívá i jiných možností, jak lépe utajit text, tak základ zůstává stejný. (Vondruška, 2006, s. 197–201)



Obrázek č. 2 – Polybius

Dalším mezníkem byla římská kultura a její nezpochybnitelný přínos pro kryptografii. První zmínky o šifrování z doby starého Říma máme od Gaia Julia Caesara, který ve své knize *„Zápisky o válce galské“* popisuje, jaké metody se k šifrování používaly. Sám Caesar používal několik šifer, které postupně zdokonaloval. Jeho šifru (jediná, která se dochovala), známe od životopisce Suetonia. Ten ve svých spisech uvedl, jak šifra fungovala. U této šifry šlo o jednoduchý posun písmen o tři pozice. Suetonius také popisuje, jak Augustus přejal od Caesara jeho šifru a upravil ji tak, že posun písmen byl jen o jednu pozici a že písmeno X nahradil písmeny AA. (Vondruška, 2006, s. 201–202), (Singh, 1999, s. 9–14), (Lunde, 2013, s. 102–104)



Obrázek č. 3 – Gaius Julius Caesar

Obrázek č. 4 – Gaius Octavianus (Augustus)

Středověk znamenal pro kryptografii úpadek, jelikož byla velmi nízká gramotnost obyvatelstva a šifry se staly výsadou příslušníků šlechty, církve a později měšťanů. V tomto období šifry vycházely z předešlých šifrových systémů. Velký přínos dal v 15. století kryptografii Leon Battista Alberti. Tento italský architekt použil systém Caesarovy šifry a upravil ho. Využil klasickou abecedu, jak ji známe dnes, a písmena zpřeházel podle předem domluveného systému a poté se celá nová abeceda posune o jednu pozici doleva, nebo doprava. Později se pro tento způsob luštění používalo posuvného pravítka. (Janeček, 1998, s. 16–17)

Obrázek č. 5 – Leon Battista Alberti

Po tomto úpadku ve středověku nastává velký rozvoj, a to v období novověku. S rozvíjejícími se vědami, diplomacií a také válečnictvím se objevuje velká potřeba utajit důležité, či strategické informace. Za zakladatele kryptografie je považován Johannes Trittheim, jenž byl opatem v benediktýnském klášteře ve Spannheimu. On sám vydal dílo zabývající se kryptografií, avšak předstihl svoji dobu a jeho dílo bylo veřejně páleno. Vymyslel tzv. tří číselnou substituci, kterou tvořily číslovky 1, 2, 3 a jejich různé kombinace, které se posléze přiřadily k písmenům abecedy. (Janeček, 1998, s. 17)

Obrázek č. 6 – Johannes Trittheim

Jedním z významných přínosů ve vývoji kryptografie bylo vynalezení tzv. mřížek. Tento princip šifrování vymyslel italský matematik, fyzik a filozof Hieronymus

Cardanus. Ve svém díle „De subtilitate“, které dokončil v roce 1550, popisuje výrobu a také princip šifrování pomocí mřížky. Tento systém spočívá v tom, že si člověk vezme papír (pergamen) a naznačí si na něj řádky. Do těchto předem nachystaných řádků si náhodně vyřeže náhodný počet čtverečků (okének). Takto upravený papír (mřížku) přiloží na druhý papír a do prázdných okének vepíše obsah zprávy (do každého okénka jedno písmeno) a zbytek řádku vyplní náhodnými písmeny. Tímto systémem mřížky se později zabýval nespočet kryptografů, avšak se zásadním vylepšením přišel až v 19. století rakouský důstojník Eduard Fleissner von Wostrovitz, který mřížku upravil na otočnou. (Janeček, 1998, s. 17–18)

Obrázek č. 7 – Hieronymus Cardanus

Koncem 16. století vznikl ve Francii nový systém šifrování. Tato šifra nese jméno svého tvůrce, kterým byl francouzský diplomat Blaise Vigenére. (Burda, 2015, s. 18–20). Tato šifra využívá buď tzv. periodické heslo, nebo tzv. autokláv. Autokláv spočívá v tom, že za dohodnuté heslo píšeme otevřený text ještě jednou, ovšem s určitým posunem, tedy máme k dispozici potenciálně neomezeně dlouhé heslo. Tato šifra vychází z ukázky nalevo.

Obrázek č. 8 – Blaise Vigenére

	A	**B**	**C**	**.....**	**X**	**Y**	**Z**
A	A	B	C	.....	X	Y	Z
B	B	C	D	.....	Y	Z	A
C	C	D	E	.....	Z	A	B
.....	.....	.....	.....	.....	.....	.....	.....
X	X	Y	Z	.....	U	V	W
Y	Y	Z	A	.....	V	W	X
Z	Z	A	B	.....	W	X	Y

Zkrácená verze Vigenérovi tabulky

Jak je z této tabulky patrné, tak pro zašifrování textu bylo mnoho možností, když je pro každé písmeno k dispozici celá abeceda. K zašifrování textu je však nutné předem domluvené heslo, podle kterého se následně šifruje. Při tvorbě zašifrovaného textu se sčítá písmeno otevřeného textu s písmenem z hesla. Podobný princip má Polybiův čtverec. Pro příklad si zvolíme, že otevřený text začíná na písmeno B a heslo taktéž. Jak je vidět již v tabulce, na souřadnici BB, je písmeno C a to by byl první znak šifrovaného textu. Dále se postupuje pořád stejně. Tento typ šifry

považovali francouzští kryptografové za nerozluštitelný, nicméně ještě před vypuknutím prusko-francouzské války se pruskému důstojníkovi podařilo šifru prolomit. (Janeček, 1998, s. 20–21)

Zásadně se na vývoji šifrování podílel také francouzský kardinál a státník Armand-Jean du Plessis Richelieu. Tento státník využil horizontální transpoziční šifry, kterou sestavil podle hesla 53142. Princip fungoval jednoduše. Otevřený text se rozdělil na skupiny po 5 znacích. Pro lepší pochopení jsem zvolil praktickou ukázku. Máme slovo JAKUB a heslo 53142. Podle tohoto je k číslici 1 přiřazeno písmeno K, k číslici 2 je B, atd. Do šifry se otevřený text převede tak, že se text přepíše od 1 do 5 popořadě. V tomto případě nám vznikne KBAUJ. Tento typ šifer se v některých evropských a některých afrických zemích používal do konce 20. století. (Janeček, 1998, s. 19–20)

Obrázek č. 9 – Armand-Jean du Plessis Richelieu

Obrázek č. 10 – Francis Bacon

Velký přínos do oblasti kryptografie přinesl lord Francis Bacon. Vymyslel systém šifrování, který dostal název „Binární šifrování“. Princip spočíval v tom, že každý znak abecedy se skládal z pěti znaků písmen A a B v různých kombinacích. Tímto systémem položil základy novodobé kryptografie. (Janeček, 1998, s. 22)

Později ve Francii vznikla šifra dvojité substituce, tzv. BIFID. Tuto šifru vymyslel Francouz Delastelle. Pro tento systém šifry je nutné mít substituční tabulku na bázi Polybiova čtverce. Následně se však zápis liší a to tím, že se píše pod sebe na dva řádky. Text by se měl rozdělovat na lichý počet znaků, kvůli pozdějšímu šifrování.

	1	**2**	**3**
1	Š	R	D
2	F	A	–
3	I	B	–

Náhodně zvolená substituční tabulka

Š	**I**	**F**	**R**	**A**	**–**	**B**	**I**	**F**	**I**	**D**
1	3	2	1	2	–	3	3	2	3	1
1	1	1	2	2	–	2	1	1	1	3

První krok šifrovaného textu

Následně se zvolí jedna možnost, jak udělat resubstituci. Možností je více, ale pro příklad zvolím tu nejjednodušší.

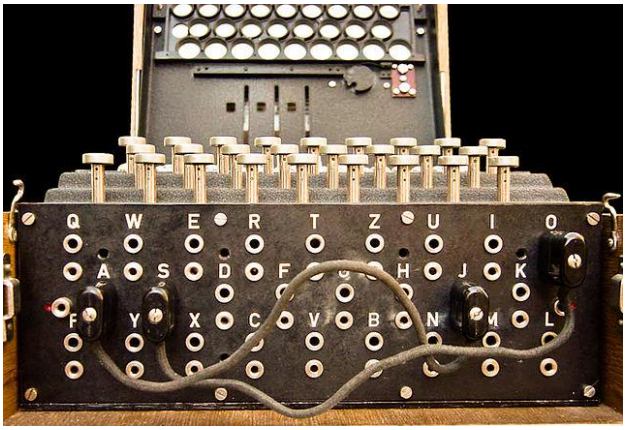
Š	I	F	R	A
1	3	2	1	2
→1	1	1	2	2

V tomto kroku se začnou psát dvojice čísel, které začínají na prvním řádku prvního slova a pokračují na řádku druhém stále první slova. Vznikne tedy druhá substituce, která vypadá takto:

13	21	21	11	22
D	F	F	Š	A

Poté se teprve šifra zapisuje. Při dešifrování dochází k opačnému procesu. (Janeček, 1998, s. 27–28)

Koncem 19. století se kryptografie upíná již novým směrům. Vychází sice pořád z předešlých typů šifer a přidává i nové, ale hlavně se šifruje a dešifruje jiným způsobem. V této době potřeba šifer na tolik složitých, aby nebyla vyzrazena strategická tajemství, a to si vyžádalo právě pomoc šifrovacích strojů. Jejich pomocí se daly šifrovat zprávy daleko efektivněji. Pro nás nejznámější byl německý šifrovací stroj ENIGMA. (Janeček, 1998, s. 34), (Lunde, 2013, s. 116–118)



Obrázek č. 11 – Šifrovací stroj ENIGMA

1.2 Kryptografie

Tato věda se zabývá utajením otevřeného textu (původní zpráva připravená k zašifrování) pomocí nejrůznějších šifer, které obsah zprávy ukryjí před případným zachycením zprávy třetí osobou. Kryptografie je podle mého názoru nejdůležitější z výše jmenovaných věd, jelikož bez jejího přičinění by texty nebyly tajné. Jak již bylo zmíněno v historickém vývoji šifrování zpráv, tak šlo šifrovat text hned několika způsoby. Těmi nejjednoduššími metodami je šifrování pomocí substituce, transpozice a kódové knihy. (Vondruška, 2006, s. 8–9)

1. **Substituční šifra** – je šifra, která dané písmeno abecedy nahradí nějakým znakem, symbolem, písmenem nebo číslem. Tuto šifru například využíval slavný římský vojevůdce Gaius Julius Caesar. Podobné této šifře jsou také substituční kódy, jako například Morseova abeceda, nebo také Braillovo slepecké písmo, jejich účel je ale jiný než u šifry, nejde zde o utajení, ale o přizpůsobení znaků způsobu přenosu, což je například u Morseovy abecedy telegrafní vysílání přerušovanou rádiovou vlnou, nebo u Braillova písma systém výstupků rozpoznatelný hmatem. (Janeček, 1994, s. 73–76), (Vondruška, 2006, s. 29)
2. **Transpoziční šifra** – tato šifra využívá jednoduchého posunu písmen na jinou pozici. Pro lepší představu lze tuto šifru předvést na příkladu SLOVO, jehož transpozicí může být OVOLS. Toto napsání pozpátku je nejjednodušší transpozice, avšak může být i složitější, kdy pořadí písmen může mít nějaký svůj řád, i přesto je tento způsob šifrování, spolu se substitucí považován za lehce prolomitelný. (Vondruška, 2006, s. 30), (Janeček, 1994, s. 25–29)
3. **Kódová kniha** – tento druh šifry funguje, již podle názvu, pomocí kódové knihy, která obsahuje slova a k nim přiřazené kódy, které mohou být ryze náhodné, tudíž hůře rozluštitelné, nebo mohou mít nějaký svůj systém, například slova začínající na písmeno G, by mohla začínat na stejnou číslici, to samé by mohlo být provedeno u samohlásek. Nicméně takovýto systém by byl lehce prolomitelný. Tento způsob zašifrování ať tak, či tak by byl velmi zdlouhavý. (Vondruška, 2006, s. 30–31), (Janeček, 1994, s. 132)

Díky neustálému soupeření kryptografů s kryptoanalytiky se kryptologie vyvíjela směrem ke složitějším a především obtížněji luštitelným šifrám. Již ve středověku se jako prvky ztěžující rozluštění textu objevují tzv. klamače, či tzv. homofony. Jen o něco později se objevuje využití polygramů.

1. **Klamač** – klamač mohl být cokoliv, avšak nenesl žádný význam a měl jen jedinou funkci, a to zmást toho, kdo se snažil šifru prolomit. (Vondruška, 2006, s. 12)
2. **Homofony** – jsou skupiny znaků šifrové abecedy, které alternativně (tzn. vždy jen jeden z nich) nahrazují jeden ze znaků otevřené abecedy, typicky se objevují u samohlásek, aby se zabránilo jejich snadné identifikaci díky vysoké frekvenci v textu. (Vondruška, 2006, s. 32)

3. **Kód** – je šifrový znak, který nahrazuje často používané slovo, sloveso atd. (Vondruška, 2006, s. 16–17)
4. **Nomenklátor** – šifrový systém kombinující homofonní substituci s klamači a kódy. (Singh, 2009, s. 43–44), (Singh, 1999, s. 41)
5. **Polygram** – „Polygram je tvořený blíže neurčeným počtem po sobě jdoucích písmen v textu.“ Velmi často jsou využívány v šifrovaných textech bigramy, které mohou být jakákoliv dvojice sousedních písmen. Taktéž jsou složené trigramy, u kterých, jak název napovídá, se jedná o písmena tři. (Vondruška, 2006, s. 13)

Vzhledem k tomu, že substituční šifra byla velice oblíbená, tak byla různě vylepšována, aby se ztížila možnost jejího rozluštění třetí osobou. Vzniklo proto hned několik typů substitučních šifer.

1. **Monoalfabetická šifra** – neboli jednoduchá substituce. Tato šifra pracuje, jak jsem již vysvětlil u pojmu substituční šifra, se záměnou písmeno → symbol/znak/číslice. Na tuto šifru lze uplatnit frekvenční analýzu k jejímu rychlejšímu prolomení. (Vondruška, 2006, s. 31)
2. **Homofonní šifra** – U této šifry nelze tak účinně pracovat s frekvenční analýzou, protože jedno písmeno v otevřeném textu může být zaměněno hned několika znaky, které jsou tzv. homofony pro dané písmeno. Avšak při zkoumání většího množství dokumentů obsahujících tutéž šifru, která je v tomto případě neměnná, je větší pravděpodobnost prolomení šifry. (Vondruška, 2006, s. 32)
3. **Polyalfabetická šifra** – tato šifra je postavena tak, že každé písmeno je zvlášť zašifrováno jednoduchou substitucí, ovšem střídají se různé substituce (typicky posuvné šifry) buď podle periodického hesla, nebo s využitím autoklávu. Tento způsob byl vyvinut na základě toho, aby již nebylo možné dešifrovat text na základě frekvenční analýzy znaků. Nicméně slabinou tohoto důmyslného systému je fakt, že jde luštit „na základě analýzy vzdálenosti mezi opakováními řetězců šifrovaných znaků“, jak uvádí Vondruška.(2006, s. 32–33)
4. **Bigramová šifra** – jak se šifry zlepšovaly proti rozluštění frekvenční analýzou, tak se použily u výše zmíněných šifer bigramy, nebo trigramy. Šifru lze nazvat bigramovou, pokud se zaměňují bigramy otevřeného textu, za bigramy ze znaků šifrové abecedy (skupina znaků, jejíž pomocí

se text šifruje). U trigramové šifry platí stejné pravidlo, jen s tím rozdílem, že se jedná o znaky tři. (Vondruška, 2006, s. 34)

5. **Digrafická substituční šifra** – tato šifra pracuje tak, že ke každému znaku původního textu jsou přiděleny dva znaky z šifrové abecedy. Tato šifra často využívala jako šifrovou abecedu číslice. Na tomto principu funguje šifra Polybiův čtverec. (Vondruška, 2006, s. 35)

1.3 Kryptoanalýza

Tato věda pracuje již se zašifrovanými texty, u kterých se snaží zjistit původní obsah zprávy před zašifrováním. Cílem snažení této vědy je prolomit danou šifru, nebo zjisti alespoň část zašifrovaného textu pomocí nejrůznějších metod, např. frekvenční analýzy. Dále se tato věda zabývá vývojem metod vedoucích k prolomení šifry, odolností šifer, zkoumá, jaká je obtížnost jejich prolomení. K dešifrování využívá i znalosti již používaných šifer. Dnes se kryptoanalýzy využívá k rozluštění dávno zapomenutých jazyků (Janeček, 2006, s. 15), (Vondruška, 2006, s. 9)

1.4 Steganografie

Tento vědní obor vznikl až později, jelikož byl často kryptografy opomíjen, nicméně samotná steganografie vznikala souběžně s potřebou ukrývat důležité zprávy. Cílem steganografie je ukrýt samotnou existenci zprávy, nikoli jen její obsah, jako tomu bylo u kryptografie. K utajení zpráv byl využit například neviditelný inkoust, nebo zpráva v obrázku. Dále, jak uvádí Singh, se text mohl ukrývat ve vejci, pokud byl dodržen určitý postup, mohl být též vyškrabán do dřeva a zalit voskem nebo vytetován na hlavu. (Singh, 2009, s. 19–21), (Singh, 1999, s. 5–7)

2 Microsoft Excel

K úspěšnému dokončení této práce bylo nutné zvolit program, který by byl vhodný na práci s velkým množstvím dat a s možností individuální úpravy těchto dat. Microsoft Excel 2007 odpovídal skvěle těmto požadavkům.

Program Excel je tabulkový procesor vyvinutý firmou Microsoft. V roce 1985 vznikl, tehdy ještě tabulkový kalkulátor, pouze pro platformu Macintosh. Až v roce 1987 byl vyvinut Excel 2.0 pro PC verzi s operačním systémem DOS 3.0. Již v roce 1983 se podařilo implementovat makra do programu Lotus 1-2-3, který tímto krokem

získal náskok nad konkurencí, jelikož nabízel možnost psaní a rovnou i testování vzniklých maker. Microsoft přidal svá makra už do verze 2.1 a postupně je vylepšoval. Později už Excel nabízel tolik možností a tolik funkcí, že bylo pro Lotus obtížné konkurovat. Vývojáři programu Lotus doufali, že systém OS/2 nahradí Windows, a proto přizpůsobili Lotus tomuto systému. Nicméně to, v co doufali, se nestalo. Microsoft se svým OS Windows se velmi brzy pevně zachytil na vedoucí pozici a se svojí sadou MS Office získal prvenství na trhu, díky čemuž Lotus 1-2-3 už neměl šanci dostat se na vrchol. V roce 1993 Microsoft sjednotil programovací jazyky z aplikací v sadě Office a tímto vlastně vznikl nový programovací jazyk s názvem Visual Basic for Applications (dále jen VBA). Tento jazyk vznikl již ve verzi s názvem Excel 5. Později vznikaly další verze jako Excel 7, Excel 97 nebo Excel 2000. Významným zlomem bylo vydání verze Office 2007, která přinesla nejvíce změn. Poté vyšly ještě další verze jako Office 2010, 2013 nebo 2016. *Microsoft Excel* [online, cit. 24. 4. 2017], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Microsoft_Excel>

Ve své práci se též zabývám VBA. Vzhledem k tomu, že množství dat bylo poněkud rozsáhlé, bylo využití maker zcela nezbytné, jelikož makra zvládají, pokud jsou efektivně napsána, poměrně rychle dešifrovat text, kteréhož šifra byla již předtím prolomena (alespoň částečně). Nejprve je nutné si definovat, co vlastně bude potřeba. V tomto případě je to procedura, pro kterou je vyhrazeno klíčové slovo „`Sub`“. Každá tato procedura začíná „`Sub názevprocedury`“ a končí kódem „`End Sub`“. (Černý, 2008, s. 60) Dále bylo nezbytné použít nějaké proměnné, protože jak je dále v práci zřejmé, šifry byly psány v řádcích, proto byly vloženy též do řádků. Proměnná se deklaruje libovolným písmenem, nebo skupinou písmen a číslic začínající písmenem (identifikátorem), ke kterému se přidá operátor „=“ a přiřadí hodnota. Ve svých makrech jsem vystačil s proměnnými označenými jedním písmenem. Použití proměnné tedy vypadá následovně: „`x = 15`“. U proměnných se dá deklarovat datový typ, ale ve VBA to není povinné. Pro tuto práci bylo též nezbytné využití výrazů a to pomocí operátorů. V práci jsem použil několik druhů operátorů, a to především aritmetické, srovnávací a logické. Aritmetické provádějí matematické operace, zahrnují například „+“, „/“ a další. Funkci srovnávacích operátorů jsem použil též mnohokrát (patrně nejčastěji používaný operátor) a do této sekce patří větší, menší, rovná se, nerovná se, větší nebo rovno nebo menší nebo rovno. Poslední logické jsem využil čistě u podmínek, pro které bylo nutné do jedné podmínky zahrnout více argumentů. (Černý,

2008, s. 66–67) Dále jsem v práci použil příkaz „`If`“, který se používá pro větvení kódu. Tento kód však nejde použít samotný, vždy musí následovat další potřebné části podmíněného příkazu. Toto větvení se proto musí skládat z „`If`“, dále pak nějaký logický výraz představující podmínku, následuje slovo „`Then`“, po kterém se uvede obvykle příkaz, který se vykoná, když je podmínka splněna. Využít lze též části „`Else`“, která nabízí druhou možnost větvení, pokud podmínka splněna není a je nutné, aby se vykonal nějaký jiný příkaz. Další možností je vložení tzv. „podpodmínky“ s názvem „`ElseIf`“, která usnadňuje a zkracuje zápis další podmínky do podmínky. Podmínka je vždy ukončena podobně jako procedura, tedy „`End If`“. (Laurenčík, 2011, s. 27) Všechny tyto kroky, popsané výše, by takřka neměly smysl, pokud by nebylo možné je používat opakovaně jejich zapojením do cyklů. Pro cyklus je zde slovo „`For`“. Tento cyklus opakuje daný počet kroků do doby, dokud je všechny neprovede, nebo do doby, kdy ve vnitřní části cyklu dojde k chybě. Pro zápis je nutné zadat název tzv. řídící proměnné a počet opakování (od – do) a cyklus ukončit slovem „`Next`“. Celý cyklus pak vypadá takto: `For názevproměnné=1 to 20` -> následuje obsah cyklu a posléze se ukončí „`Next názevproměnné`“. Název řídící proměnné cyklu se používá i při ukončení pro lepší přehlednost, avšak není zde nezbytný. (Laurenčík, 2011, s. 37–38) Pro práci s buňkami lze použít slovo „`Range`“, avšak já jsem ve svých makrech použil alternativu „`Cells(x, y)`“, kde slovo „`Cells`“ označuje buňku a „`x`“ a „`y`“ souřadnice, kde se nalézá. Díky tomu, že bylo možné přesně specifikovat konkrétní buňky, tak jsem provedl grafické úpravy dešifrovaného textu. VBA nabízí totiž širokou škálu možností, jak lze upravovat buňky. Lze zde upravit například velikost písma, barvu písma, barvu pozadí buňky, styl písma, zarovnání a další. Zde jsem stručně popsal všechny funkce, které jsem v MS Excel využil a upravil, podle svojí potřeby. (Laurenčík, 2011, s. 49–53), (Weber, Breden, 2007, s. 37–38)

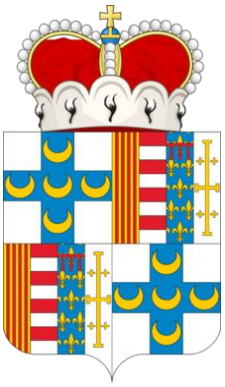
3 Piccolominiové

Obrázek č. 12 – Rodový erb Piccolominiů

Je to starý italský prominentní rod, který se datuje již od 13. století. Svoji působnost a věhlas rozšiřovali z jejich rodného města Siena. Tento rod se již od počátku snažil, a úspěšně, získávat bohatství. Jedním z úspěšných kroků bylo, že získal panství Montertari za svoji podporu císaři Fridrichu II. Ve svém rodném městě dále členové rodu rozšiřovali majetek a stavěli si zde domy a věže, které měli odrážet prestiž jejich rodiny. Svoji působnost však nezaměřovali pouze na město Siena. Díky obchodu, který v této zemi vzkvétal, měli možnost svoje obchodní zájmy přesunout i do jiných italských měst, zejména do Benátek a Janova, kde si stavěli obchodní domy. Jejich, zejména obchodní, vliv sahal až do některých německých a francouzských měst. Piccolominiové se zapletli do mocenského konfliktu Guelfů a Ghibellinů a za vlády sicilského krále Manfréda byli vyhnáni z města a jejich domy byly vypáleny. Po nějakém čase se opět mohli vrátit do rodné Sieny díky podpoře neapolského krále Karla I. z Anjou. Avšak i když si zachovali větší část svého panství, jejich vliv upadl a přešel do města Florencie. Část jejich rodu se přesunula do Neapolského království, kde se úspěšně stala jedním ze sedmi vládnoucích rodů v zemi. Z rodu Piccolominiů vzešlo mnoho významných osobností, mimo jiné dokonce dva papežové. Prvním z nich byl Enea Silvio Piccolomini, jenž přijal jméno Pius II. Druhým papežem z jejich rodu byl Francesco Piccolomini, který přijal jméno Pius III. Za zmínku stojí rovněž Antonio Piccolomini, první Vévoda z Amalfi. Antonio jako první získal titul vévody a byl zároveň synovcem papeže Pia II. a bratrem papeže Pia III. Dalšími významnými členy byli Girolamo Piccolomini junior a senior, oba získali titul biskupa z Montalcina a Peinzy. Co se týče církve, tak z tohoto rodu pocházejí ještě dva Piccolominiové a to Ascanio I. a II. Piccolomini, kteří byli arcibiskupové ve městě Siena. Jedním z posledních nejslavnějších Piccolominiů byl Otavio Piccolomini, který se nejvíce proslavil ve třicetileté válce. Poslední významný Piccolomini byl Enea Silvio, který byl říšským generálem ve válce proti Turecku. *Piccolomini* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Piccolomini>

3.1 Otavio Piccolomini

Otavio (či Ottavio, nebo Oktavio) Piccolomini byl italský generál, který ve službě Svaté říše římské dosáhl hodnosti polního maršála. Také byl zapleten do vraždy Albrechta z Valdštejna, který byl nejvyšším velitelem císařských vojsk a získal titul generalissimus. *Albrecht von Wallenstein* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Albrecht_von_Wallenstein>, *Ottavio Piccolomini* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Ottavio_Piccolomini>



Obrázek č. 13 – Rodový erb Otavia Piccolominiho

Otavio se narodil 11. listopadu 1599 ve Florencii. V 16 letech dokončil vojenskou školu a nastoupil na vojenskou kariéru. Ještě před vypuknutím třicetileté války byl povýšen do hodnosti kapitána kavalerie v Čechách, kam ho poslal v císařských službách toskánský vévoda. Následně se zúčastnil bitvy na Bílé Hoře. Poté se na nějaký čas připojil do španělské armády jako kyrysník v hodnosti podplukovníka. Jeho velmi rychlý kariérní postup byl zapříčiněn také tím, že jeho rodina byla velmi úzce svázána s papežským stolcem a mnoha biskupy a arcibiskupy v Itálii, kde se děla hlavní diplomatická jednání. Do říšské armády se opět vrátil již v hodnosti plukovníka a velitele Valdštejnovi osobní stráže. Otaviovi se připisuje, že byl zapletený do vraždy Albrechta z Valdštejna, nebo že o ní alespoň něco věděl, konec konců, byl velitelem jeho osobní stráže, která nebyla na svém místě. V hodnosti plukovníka se zúčastnil bitvy u Lützenu, za kterou dostal hodnost polního maršála (dnes by to byl generálmajor). V třicetileté válce ještě vyhrál, ale i prohrál mnoho bitev, avšak byl se svojí hodností nespokojen. Po smrti Petra Malandera, hraběte z Holzapfelu, byl jediný, kdo nesl takto vysokou hodnost, tudíž po jeho smrti se stal de facto generalissimem. Nicméně krátce na to císař uzavřel mír a poslal mu děkovný dopis a 114 566 guldenů. Poté se Otavio usadil na panství v Náchodě, které spolu s dalšími získal v českém království za věrnou službu říši. (Wachsmannová, Blažková, 1958, s. 14), *Ottavio Piccolomini* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Ottavio_Piccolomini>

Obrázek č. 14 – Podobizna Otavia Piccolominiho

3.2 Návštěva SOA Zámrsk

Tématem práce jsou historické šifry a jejich analýza, takže bylo nutné si nějaké opatřit. Na doporučení vedoucího práce jsem se vydal do Státního Oblastního Archivu v Zámrsku. Po předchozí korespondenci s archivem mi bylo nejprve sděleno, že se tam žádné dokumenty s šiframi nevyskytují, avšak přesto jsem se se svým kolegou, bývalým studentem historie na UHK, vydal do zmiňovaného archivu. Sám archiv se nachází v rekonstruovaném zámečku v Zámrsku. Můj kolega mne upozornil, že zde badatelna bývá často plná, takže bylo nezbytné tam být již kolem 8:00, kdy se badatelna otevírá. Naneštěstí bylo ten den méně než -20°C, a nebýt milého kolektivu archivu, museli bychom mrznout venku mnohem delší dobu. Hned při vstupu mne ohromil stav, v jakém se zámeček nachází. Z archivních fotografií byl ve velmi žalostném stavu a nyní je opravdu skvostný. Po příchodu do vstupní místnosti badatelny jsem byl ohromen vybaveností této odpočinkové místnosti, protože jsem měl srovnání se SOkA Havlíčkův Brod, kde jsem se též (mimo téma této práce) zabýval starými texty. Bohužel jsem neudělal pro lepší představu fotografie, protože jsem to nepovažoval za přínosné k této práci. Po vstupu do samotné badatelny jsem byl požádán, abych vyplnil badatelskou kartu (spíše takový dotazník) a již dopředu jsem měl nachystané archivní pomůcky k rodinnému archivu Piccolominiů. Samotných pomůcek bylo hned několik. Jedna část se zabývala přímo texty a část druhá je uskupovala do mikrofilmů v určitém intervalu inventárních čísel. Ke každému dokumentu v obou druzích pomůcek byl popis. Vzhledem k tomu, že bylo nutné nalézt konkrétní dokumenty, tak jsme museli s kolegou projít každý více jak dva tisíce stránek, přičemž jsme hledali dokumenty bez popisu, protože ty by byly v šifrách a nebyly by rozluštěny. Nicméně se to nestalo a požádali jsme paní v badatelně, jestli by nám mohla donést konkrétní mikrofilm. Následně nás zavedla do vedlejší místnosti, kde nám vysvětlila práci s promítačkou a my jsme prohlíželi snímek po snímku v období třicetileté války v životě Otavia Piccolominiho. Asi po padesáti snímcích se objevila první šifra. Celkem jich na tomto mikrofilmu bylo přes dvacet. Avšak mikrofilm brzy skončil. Proto jsme si s kolegou řekli, že bychom jich mohli zkusit více a získat proto další dokumenty k budoucí práci. Druhý mikrofilm obsahoval tolik šifer, že jsme je ani všechny nemohli zdokumentovat, protože byl čtvrtek a úřední hodiny badatelny jsou jen do 15:00. Tento druhý mikrofilm obsahoval přibližně čtyřicet snímků s šiframi, ale jsem si jistý, že by jich zde bylo mnohem víc. Dále jsem přesvědčen, že se šifry nalézají i na jiných mikrofilmech. Nicméně

mikrofilmů jsou desítky a celkový počet snímků ve většině případů přesahuje číslo 50. Hledání může usnadnit na první pohled velmi zmatená systematika, protože vše se zakládá na inventárních číslech, ale nakonec si člověk musí ať tak, či tak najít konkrétní mikrofilm. V našem hledání jsme dlouho nemohli zjistit, jaký mikrofilm zvolit, ale po jedné indicii v archivní pomůcce, kde se psalo „obsahuje šifru“ (to byl jediný dokument, který obsahoval tuto indicii), jsme zjistili inventární číslo dokumentu. Poté v jiné archivní pomůcce (ta která se zabývá mikrofilmy) jsme si našli číslo filmu, v jehož intervalu inventárních čísel je naše inv. číslo. Následuje vyplnění žádanky a člověk dostane mikrofilm. Druhý mikrofilm byl hned číslo po tomto. Tímto postupem jsem pro potřeby této práce získal dostačující počet dokumentů, kterými jsme se mohli s vedoucím práce zabývat. Práce s dokumenty v tomto archivu byla pro mne velmi obohacující, jelikož mým druhým oborem zde na UHK je historie a také proto, že lidé, i prostředí kolem, byli velmi příjemní a nápomocní.

4 Zašifrované dokumenty

4.1 Šifra v dokumentu 25039

Tabulka č. 1 – Dešifrovací tabulka

X	1	2	3	4	5	6	7	8	9
1	a		b	u	c		d	que	f
2	e		g	et	l		a	e	l
3	i		m	sko	n		p		q
4	o		r	tre	s		t	m	o
5	u				y		s		
6	a	a	g		e		i		l
7	n		o		r		s	rc	t
8	u			–		–	e	–	
9	e		n				r		

Jak již bylo zmíněno v historii kryptografie, byl v této šifře Otavia Piccolomini použit systém Polybiova čtverce. U této tabulky je patrné, že na rozdíl od Polybia, Otavio neobsadil všechna pole tabulky, a proto tu jsou i čísla, která se v zašifrovaných zprávách nevyskytují. Těmito čísly jsou například 22, 32 apod. Z této tabulky můžeme též zjistit, že Otavio volil souřadnice pro souhlásky převážně v lichých sloupcích. Často používaná slova, v tomto případě zkratky nahradil nomenklátory a umístil je do sudých sloupců. V sudých sloupích se vyskytují i samostatná písmena, to bylo nejspíše z důvodu potřeby většího zabezpečení šifry, vzhledem k Otaviově postavení. V šifře se také objevují klamače, pro které autor zvolil číslovky 84, 86 a 88. Následuje přepis šifry samotné i s mezičádkovou kryptoanalýzou, ze které plyne, že v tomto případě byl zašifrován otevřený text ve francouzštině. Dvojice číslic představují šifru, zvýrazněný text dešifrovanou část.

15 21 45 47 14 71 65 33 31

c e s t u n e m i

45 21 43 65 18 45 55 35 41 14 77 37 41 14 97 31 73 71 45 84

s e r e que s y n o u s p o u r i o n s –

35 41 51 45 21 71 44 47 61 35 67 43 86

n o u s e n tre t a n i r –

14 71 33 41 31 77 21 35 15 21 15 11 33 37

u n m o i s e n c e c a m p

31 41 67 23 71 61 93 47 37 43 21 45 18 29 21 69 87 14 43

i o i g n a n t p r e s que l e l e u r

29 11 17 31 47 87 61 97 33 21 21 88 86 21 35 35 65

l a d i t e a r m e e – – e n n e

33 55 21 45 21 43 41 31 47 43 21 17 51 31 47 65

m y e s e r o i t r e d u i t e

11 29 61 43 51 55 71 21 31 29 35 41 51 45

a l a r u y n e i l n o u s

19 11 51 88 17 97 62 11 19 62 81 47 21 17 51 71 21

f a u – d r a a f a u t e d u n e

44 21 47 11 31 35 65 17 21 33 31 29 37 11 47 11 15

tre t a i n e d e m i l p a t a c

41 71 77 37 49 51 43 19 86 11 31 75 21 29 11 37 43 41 51

o n s p o u r f – a i r e l a p r o u

31 45 31 41 35 84 88 35 21 15 65 45 77 11 31 43 21 17 21 29 11

i s i o n – – n e c e s s a i r e d e l a

37 43 88 41 51 31 11 35 63 21 29 61 39 81 21 69 91 65 71 41 14 77

p r – o u i a n g e l a q u e l e e n o u s

33 11 35 84 86 15 39 81 21 37 43 21 35 17 75 65

m a n – – c q u e p r e n d r e

61 81 47 97 27 84 43 65 45 41 88 29 51 47 31 41 71

a u t r a – r e s o – l u t i o n

11 35 41 51 45 21 45 29 41

a n o u s e s l o

31 23 15 86 65 97 17 65 39 81 65 29 18 69 31 63 51 65 45

i g c – e r d e q u e l que l i g u e s

17 31 15 55 41 51 71 41 51 45 37 14 31 45 77 67 73 71 77

d i c y o u n o u s p u i s s i o n s

48 51 14 21 75 29 65 45 17 31 47 57 51 88 86 67 81 43 21 77

m u u e r l e s d i t s u – – i u r e s

24 19 41 51 86 84 43 11 23 21 45 11 19 31 35

et f o u – – r a g e s a f i n

17 21 35 21 14 41 31 43 15 14 39 51 21 17 31 21 14

d e n e u o i r c u q u e d i e u

35 21 37 29 11 31 45 21 43 21 17 51 31 15 47 21

n e p l a i s e r e d u i c t e

15 65 47 79 65 13 21 69 91 21 61 43 33 21 65 21 71

c e t t e b e l e e a r m e e e n

47 87 91 21 45 47 11 79 33 31 45 21 75 11 13 29 21

t e e e s t a t m i s e r a b l e

15 41 33 33 21 65 69 69 87 45 11 48 51 81 21

c o m m e e l l e s a m u u e

17 51 37 11 45 45 21 11 51 15 61 33 34

d u p a s s e a u c a m sko

37 43 41 15 25 21 13 21 43 65 35 13 41 51 43 23

p	**r**	**o**	**c**	**l**	**e**		**b**	**e**	**r**	**e**	**n**	**b**	**o**	**u**	**r**	**g**
21	35	39	51	41	55		15	41	35	45	31	45	47	28		
e	**n**	**q**	**u**	**o**	**y**		**c**	**o**	**n**	**s**	**i**	**s**	**t**	**e**		
35	21	11	35	47	33	41	31	71	45		29	11				
n	**e**	**a**	**n**	**t**	**m**	**o**	**i**	**n**	**s**		**l**	**a**				
15	41	35	84	45	21	43	51	11	47	31	41	35		73	51	
c	**o**	**n**	**–**	**s**	**e**	**r**	**u**	**a**	**t**	**i**	**o**	**n**		**o**	**u**	
37	21	43	47	21		17	51	43	21	45	47	21		17	21	
p	**e**	**r**	**t**	**e**		**d**	**u**	**r**	**e**	**s**	**t**	**e**		**d**	**e**	
29	21	33	37	84	31	43	21		63	21	17	69	51	45		78
l	**e**	**m**	**p**	**–**	**i**	**r**	**e**		**g**	**e**	**d**	**l**	**u**	**s**		**rc**

Pro samotné dešifrování této šifry byl použit následující algoritmus, který byl pojmenován „`Dekodovani`“.

```
Sub Dekodovani()

a = 25
B = 27

For F = 1 To 40
     For j = 1 To 40

          kod = Cells(a, j)
          radek = Int(kod / 10)
          sloupec = kod - 10 * radek
          pismeno = Cells(radek + 8, sloupec + 3)
          Cells(B, j) = pismeno

Cells(a, j).HorizontalAlignment = xlCenter
Cells(B, j).Interior.Color = RGB(235, 160, 35)
Cells(B, j).HorizontalAlignment = xlCenter
Cells(B, j).Font.Bold = True
Cells(a, j).Font.Size = 10
Cells(B, j).Font.Size = 10

     Next j

   a = a + 4
   B = B + 4

Next F

End Sub
```

Každé makro je nutné v MS Excel definovat. Toto definování spočívá v tom, že před názvem makra se napíše „`Sub`“ a jméno makra následované závorkami „`()`“. V těchto závorkách mohou být uvedeny argumenty, ale velmi často makra žádné argumenty nemají, takže závorky zůstanou prázdné. Každé makro musí být ukončeno „`End Sub`“.

Pro tento algoritmus jsem si na začátku zvolil dvě proměnné a to „`a`“ a „`B`“. Jejich hodnoty udávají čísla řádků v tabulce MS Excel. První hodnota je pro řádek, na kterém je šifra a ten druhý má hodnotu prázdného řádku, kam bude šifra převedena do otevřeného textu. Dalším krokem bylo vložení cyklu „`For`“, avšak pro tyto účely bylo nezbytné vložit tyto cykly dva. Každý cyklus musí být na svém konci ukončen příkazem „`Next`“ a k tomuto označení se pro přehlednost přidává jméno řídící proměnné cyklu, např. F. Uvnitř cyklu s řídící proměnnou „`F`“ se zvyšují hodnoty čísel řádků „`a`“ a „`B`“ vždy o číslo 4. To je nezbytné, aby se postupně dešifrovaly všechny řádky. Obsah cyklu „`j`“ je o něco komplikovanější. V prvním kroku se do proměnné

„kod“ nahraje obsah buňky se souřadnicemi „a“ a „j“, kde písmeno „j“ označuje číslo sloupce tabulky. Získaný kód, který představuje zpravidla jedno písmeno otevřeného textu, zašifrované pomocí dvou číslic je potřeba rozdělit na číslo řádku a číslo sloupce příslušného šifrovacího čtverce. Do proměnné „radek“ se vloží obsah proměnné „kod“ a vydělí se číslovkou 10. Tím vznikne desetinné číslo, které převedeme na „Int“ – celé číslo, a tím získáme první souřadnici pro výsledné písmeno, které je zapsáno v šifrovacím čtverci. Dalším nezbytným krokem je získání druhé souřadnice. Tu získáme tak, že do proměnné „sloupec“ nahrajeme proměnnou „kod“ a odečteme od ní desetinásobek proměnné „radek“. Tímto máme obě souřadnice, které lze nyní spojit a získat výsledné písmeno. To získáme tak, že do proměnné „pismeno“ vložíme obsah buňky, která má souřadnice „radek“ a „sloupec“, avšak zde je nutné upřesnit polohu šifrovacího čtverce, pokud písmeno na souřadnici 11 není na stejném místě i v tabulce MS Excel. Tento problém lze vyřešit, jak je vidět i v následujícím kódu, přičtením konstant tak, aby se souřadnice shodovaly. V následujícím kroku již dáme do buňky se souřadnicemi „B“ a „j“ hodnotu, která se v předešlém kroku nahrála do proměnné „pismeno“.

Kód pokračuje několika dalšími příkazy, které neprovádějí žádné matematické operace, ale pouze upravují text, aby nemusel být následně manuálně upravován. První je nastavení vlastnosti zarovnání textu `HorizontalAlignment = xlCenter`. Tato hodnota představuje horizontální zarovnání obsahu buněk na střed. Které buňky se budou upravovat, stanovuje `Cells(a, j)`, což jsou souřadnice. Druhou vlastností je `Interior.Color`, která upravuje barvu výplně určených buněk. Stejně jako u předchozí funkce, tak i zde polohu změny určují souřadnice buňky `Cells(B, j)`. U této vlastnosti je nezbytné upřesnit barvu, kterou chceme a to tak, že za tuto funkci dáme „=“ a odstín barvy, v našem případě `RGB(235, 160, 35)`. Čísla vevnitř závorky představují odstíny spektra barev RGB (red, green, blue), jejichž spojením získáme požadovanou barvu. Dále tu pak máme nastavení vlastností `Font.Bold = True` a `Font.Size = 10`. První z nich upravuje písmo na tučné, druhá mění velikost písma v buňkách na velikost 10. Po tomto kroku je nejprve dokončen vnitřní cyklus a následuje dokončení prvního kroku vnějšího cyklu.

Nyní, když už je text „čistý“, ho můžeme podrobit frekvenční analýze. Každý jazyk má určitý počet písmen, která používá častěji, která méně a která vůbec, proto výsledek frekvenční analýzy může potvrdit, či vyvrátit správné určení pozice některých

písmen v šifrovacím čtverci. Podle otevřeného textu, který je v příloze, se nechalo snadno zjistit, o jaký jazyk se jednalo – v tomto případě o francouzštinu. S využitím vytvořeného makra se realizovala frekvenční analýza a potvrdila pozici písmen v tabulce. Následující makro bylo pojmenováno „Frekvence“.

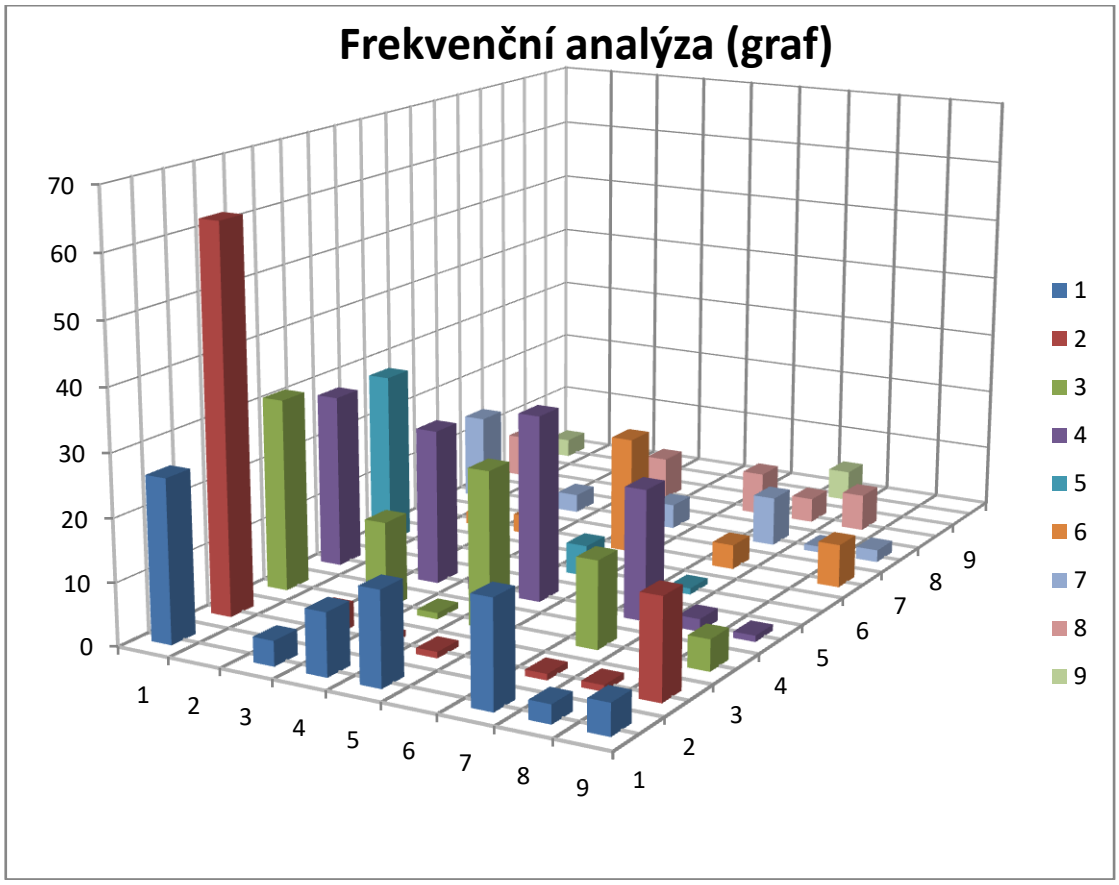
```
Sub Frekvence()

a = 25

For x = 1 To 40
     For i = 1 To 40

          kod = Cells(a, i)
          radek = Int(kod / 10)
          sloupec = kod - 10 * radek
          Cells(radek + 250, sloupec + 3) = Cells(radek +
          250, sloupec + 3) + 1

     Next i

  a = a + 4

Next x

End Sub
```

V zásadě se hlavička makra vůbec neliší, až na to, že zde nebylo nutné využití proměnné „B“, jako u předchozích maker a také se zde jmenují jinak cykly. I když jsou zde řídící proměnné cyklů pojmenovány „x“ a „i“, tak plní analogickou funkci jako v makru „Dekodovani“. Jediný rozdíl od makra „Dekodovani“ je ve vnitřním cyklu „i“. V první části probíhá vše stejně. Do proměnné „kod“ se vloží obsah buňky, do proměnné „radek“ první souřadnice a do proměnné „sloupec“ druhá souřadnice. V následujícím kroku nastává změna. Do buňky `Cells(radek + 250, sloupec + 3)`, která začíná až na řádku 250 a ve třetím sloupci vloží číslo 1 na souřadnice, kde by normálně byly na pozice písmene v dešifrovací tabulce. Vždy, když makro najde písmeno, které je obsaženo v šifrovací tabulce a má jeho souřadnice, tak přičte k hodnotě v buňce `Cells(radek + 250, sloupec + 3)` jedničku. Tímto způsobem vznikne následující tabulka, ve které můžeme vidět nejčastější písmena a pak i ta, která se nevyskytují vůbec.

Tabulka č. 2 – Frekvenční analýza

X	1	2	3	4	5	6	7	8	9
1	26		4	10	15		17	3	5
2	62		4	1	1		1	1	16
3	31		14	1	25		14		5
4	28		25	2	30		21	2	1
5	28				5		1		
6	8	2	3		19		4		7
7	14		3		4		8	1	2
8	7			7		7	4	6	
9	3		1				5		

Tato tabulka vznikla v MS Excel, kde na ní bylo použito podmínění formátování. Díky této automatické funkci Excelu je v tabulce na první pohled patrné, která písmena (když porovnáme s dešifrovací tabulkou) se v textu objevují častěji a která skoro vůbec. Díky datům získaných touto tabulkou, jsem v MS Excel vytvořil graf, na kterém se lépe projevuje spektrum používaných písmen v analyzovaném dokumentu.



Graf č. 1 – Frekvenční analýza

4.2 Šifra v dokumentu 24873

Tabulka č. 3 – Dešifrovací tabulka

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**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
–	b	c	d	–	f	g	h	–	j	k	l	m	n	–	p	q	r	s	t	–	v	–	–	–	z	a	–	e	–	i	–	o	–	u

Tato šifra používá, oproti předchozí šifře, jiný systém šifrování. Tento systém je mnohem jednodušší, protože využívá jednoduché substituce. Jak je z tabulky patrné, tak všechny samohlásky jsou nahrazeny čísly a to jen těmi lichými. Pořadí, jakým jsou přiřazené, dělají šifru ještě jednodušší pro vyluštění. Kromě samohlásek je každé písmeno na svém místě. Prázdná místa po samohláskách vyplňují pomlčky. Zde je jedna výjimka. Jelikož při dešifrování bylo zřejmé, že se jedná o italštinu, tak písmena W, X a Y mají také pomlčku, protože se v italštině nevyskytují. Následuje šifra, kde se na prvním řádku objevuje kombinace číslic a písmen a na řádku pod tím dešifrovaná část textu.

s g 1 1 l t 3 z 1 8 4 d 3 s 5

s g a a l t e z a – – d e s i

d 3 r 1 c 2 h 8 3 9 7 s t 2 r 1

d e r a c – h – e u o s t – r a

3 c c 3 l 8 3 n z 1 1 9 9 5 s 8 5 t 9 8 t

e c c e l – e n z a a u u i s – i t u – t

2 t 3 l 3 p 1 r t 5 c 7 8 l 1 r 5 t 1

– t e l e p a r t i c o – l a r i t a

p 3 r s 9 7 m 1 g 2 g 5 7 r

p e r s u o m a g – g i o r

s 7 9 3 r n 7 t 1 n t 7 n 3 l 4 l 1

s o u e r n o t a n t o n e l – l a

p 7 l 5 t 5 c 1 q 9 1 n t 7 n 3 l 2 l 1

p o l i t i c a q u a n t o n e l – l a

m 5 l 5 t 1 r 3 c 7 m 3 5 4 5 r 5 t r 7 9 5 n 7

m i l i t a r e c o m e i – i r i t r o u i n o

l 3 c 7 s 3 q 9 1 l 2 4 l 5 3 t l 3

l e c o s e q u a l – – l i e t l e

c 7 n d 5 t 5 7 n 5 d 3 4 l v l 5 m 5 n 5 2 s t r v 5

c o n d i t i o n i d e – l v l i m i n i – s t r v i

v 2 4 5 n s 7 m 1 t 9 4 t 2 2 t 7 q 9 3 7 c 2 h 4 3

v – – i n s o m a t u – t – – t o q u e o c – h – e

s 5 9 d 5 v c 1 7 p 7 r t 9 n 7 p 3 r 5 l

s i u d i v c a o p o r t u n o p e r i l

s v 8 9 3 r v n 7 c 4 2 k 3 s 1 r 5 1 p 3 r v 4 2

s v – u e r v n o c – – k e s a r i a p e r v – –

Pro dešifrování této šifry bylo použito makro s názvem „`Dekodovani`“. Tento název se sice shoduje s předešlým makrem, ale obsah makra je naprosto odlišný. V minulé šifře se pracovalo s čísly, která jdou násobit, dělit atd. V tomto případě jsem musel vytvořit zcela odlišné makro, protože zde se kromě číslic vyskytují i písmena. Problém byl v tom, že s písmeny nejdou provádět matematické operace, protože nemají žádnou početní hodnotu. Původní makro „`Dekodovani`“, které jsem proto upravil, aby bylo možné text efektivně dešifrovat.

```
Sub Dekodovani()

Ax = 12
Bx = 14

Dim kod As String

For F = 1 To 20
     For j = 1 To 50

          kod = Cells(Ax, j).Text
          Ifkod = "" Then
          Cells(Bx, j) = ""

          ElseIf kod = "a" Or kod = "e" Or kod = "i" Or kod
          = "o" Or kod = "u" Or kod = "w" Or kod = "x" Or
          kod = "y" Or kod = "2" Or kod = "4" Or kod = "6"
          Or kod = "8" Then
          Cells(Bx, j) = "-"

          ElseIf kod = "1" Then
          Cells(Bx, j) = "a"
          ElseIf kod = "3" Then
          Cells(Bx, j) = "e"
          ElseIf kod = "5" Then
          Cells(Bx, j) = "i"
          ElseIf kod = "7" Then
          Cells(Bx, j) = "o"
          ElseIf kod = "9" Then
          Cells(Bx, j) = "u"
          Else
          Cells(Bx, j) = kod
          End If

Cells(Ax, j).HorizontalAlignment = xlCenter
Cells(Bx, j).Interior.Color = RGB(235, 160, 35)
Cells(Bx, j).HorizontalAlignment = xlCenter
Cells(Bx, j).Font.Bold = True
Cells(Bx, j).Font.Size = 10

     Next j

     Ax = Ax + 4
     Bx = Bx + 4
Next F
End Sub
```

Jako i v předchozím makru, jsem si na začátek zvolil dvě proměnné s názvy „Ax“ a „Bx“, které představují řádek s šifrou a řádek, kam se bude šifra dešifrovávat. Změnou oproti předešlému makru je také definice proměnné „kod“. Tato proměnní totiž již nemůže být typu „Int“, protože pracuje i s písmeny, proto je definována jako „String“. Opět byly pro dešifrování využity dva cykly. Ten vnější, označen „F“ je úplně stejný, jen používá jiné proměnné se stejnou funkcí. Ve vnitřním cyklu „j“ se jako první nahraje do proměnné „kod“ hodnota buňky, ale jiným způsobem. Jelikož je „kod“ definován jako řetězec „String“, tak musí zápis vypadat takto: `Cells(Ax, j).Text`. Kód pokračuje jednoduchou podmínkou „If“, která se ptá, jestli je v proměnné „kod“ prázdná buňka. Pokud je, tak se nic nemění a do `Cells(Bx, j)` se vloží prázdná hodnota, stejně jako u předešlého makra. Změna nastává, pokud se tato hodnota liší. Pro tuto možnost jsem použil výraz, který podmínka podporuje a to „ElseIf“. Tento výraz neskutečně zkrátí celý kód, pokud je nutné, jako v tomto případě, použít více podmínek najednou. První část této podmínky hledá v textu samohlásky, nepoužívaná písmena a pak sudá čísla, aby je mohla nahradit pomlčkou. V dalších podmínkách se vyhledávají lichá čísla, která se po nalezení nahradí příslušnou samohláskou. Po všech těchto podmínkách následuje slovo „Else“, v češtině přeloženo „jinak“, po kterém je poslední možnost, kdy není žádná s podmínek splněna. Tato část nemusí obsahovat nic, dokonce v podmínce ani být nemusí, ale pro účely této práce tam být musí, jelikož tam přepisuje písmena, na která se podmínky nevztahují. Teprve až po tomto lze ukončit podmínku výrazem „End If“. V tomto cyklu kód ještě obsahuje úpravy textu jako „HorizontalAlignment“, „Interior.Color“, „Font.Bold“ nebo „Font.Size“. Po dokončení toho makra je text možné podrobit frekvenční analýze, jejíž kód dostal název „Frekvence“.

```
Sub Frekvence()

Ax = 12
Bx = 76

For k = 6 To 40
     Cells(Bx, k) = 0
Next k

For F = 1 To 30
     For j = 1 To 50
          For k = 6 To 40

               If Cells(Ax, j) = Cells(74, k) Then
               Cells(Bx, k) = Cells(Bx, k) + 1

          Next k
     Next j

     Ax = Ax + 4

Next F

End Sub
```

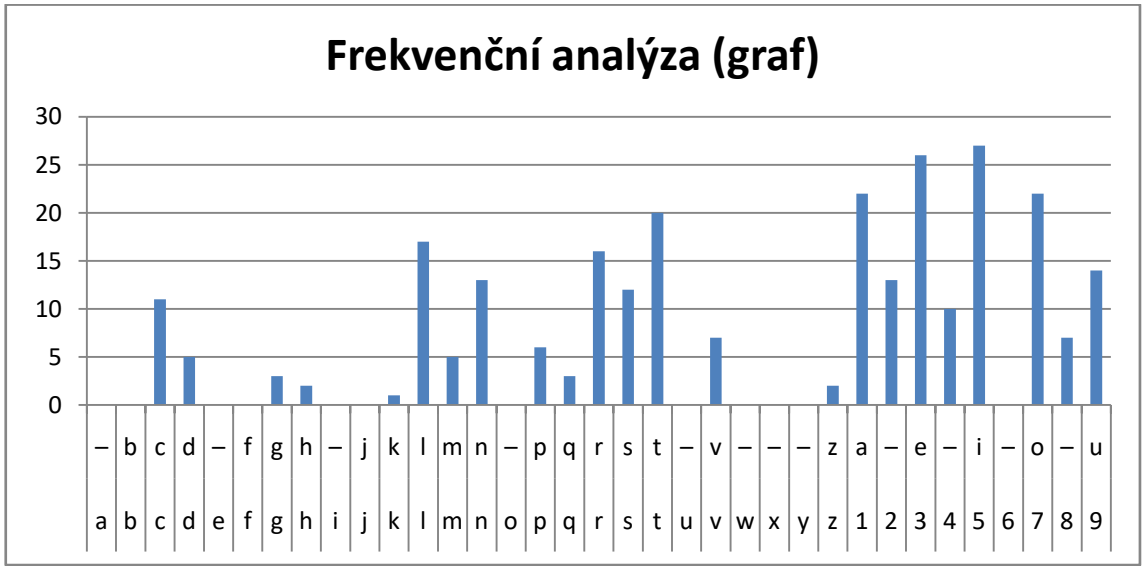
Tento kód se na první pohled jeví svojí podobností s předchozím, nicméně je od základu úplně jiný. Proměnná „Ax“ označuje řádek v MS Excel, ze kterého bude algoritmus číst hodnoty, „Bx“ označuje řádek, kam budou nové zapsány. Hned ze začátku je dobré celý řádek vynulovat a to pomocí jednoduchého cyklu „k“, následně se cyklus uzavře. Tuto možnost vynulování jsem zvážil i u předchozí frekvence, avšak při použití podmíněného formátování, kdy je v tabulce výrazné barevné spektrum, by byly přebytečné nuly matoucí. Jelikož u této šifry není možné určit souřadnice, jako tomu bylo v předchozí šifře, tak je nezbytné použít i třetí cyklus, pojmenovaný též „k“. V tomto cyklu je podmínka, která se ptá, jestli je obsah buňky na řádku „Ax“ stejný, jako obsah některé buňky v řádku 74. Jestliže se u nějakého písmene, či číslice najde shoda, tak se přičte do řádku (Bx, k) jednička.

Tabulka č. 4 – Frekvenční analýza

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	1	2	3	4	5	6	7	8	9
–	b	c	d	–	f	g	h	–	j	k	l	m	n	–	p	q	r	s	t	–	v	–	–	–	z	a	–	e	–	i	–	o	–	u
0	0	11	15	0	0	3	2	0	0	1	17	5	13	0	6	3	16	12	20	0	7	0	0	0	2	22	13	26	10	27	0	22	7	14

U této tabulky, vzhledem k její šířce, musejí být dvojice čísel pod sebou. Nejedná se o dva samostatné řádky, nýbrž o dvojice číslic – u písmena „n“ je to například číslovka 13.

Díky tabulce získaných dat bylo možné sestrojit graf, který se od předešlého grafu hodně liší a to především tím, že je v jednom sloupci, jedno písmeno. Graf vypadá přehledněji a podle frekvence používaných písmen je zjevné, že se jedná s velkou pravděpodobností o jiný jazyk než francouzština. Je vidět, že oba jazyky používají s jinou frekvencí určité samohlásky.



Graf č. 2 – Frekvenční analýza

4.3 Šifra v dokumentu 24790

Tabulka č. 5 – Dešifrovací tabulka

2	**5**	**£**	**r**	**3**	**l**	**ß**	**g**	**o**	**c-**	**c**	**4**	**s**	**+**	**&**	**d**	**ά**	**8**	**a**	**iio**	**i8.**
a	c	d	e	f	g	h	i	i	k	l	m	n	o	p	r	si	t	u	$	$$

$ iniciály jména (nečitelné)
$$ da. di Corena

U této šifry byl použit podobný systém šifrování, jako u šifry předchozí, a to jednoduchá substituce. Každý znak abecedy (v tomto případě jen některých písmen) je nahrazen znakem. Znaky v této tabulce jsou pouze náhradou za původní znaky, protože většinu znaků v textu počítač nezná. Ač jsou některé podobné, většina je zcela jiná. Dále se v textu objevují skupiny písmen, které do tabulky nezapadají a nesou zvláštní význam. S těmito skupinami byl velký problém, protože čitelnost dokumentu je místy velmi špatná a zároveň ne vždy odpovídá textu. V této tabulce jsem jen pro představu vyjmul původní znaky z dokumentu. Vynechány jsou jen poslední dvě zkratky, které by byly po vyjmutí naprosto nečitelné

2	5	£	r	3	l	ß	g	o	c-	c
a	c	d	e	f	g	h	i	i	k	l

4	s	+	&	d	ά	8	a	iio	i8.
m	n	o	p	r	si	t	u	$	$$

Je možné, že některé znaky, jako například „c-“ mohou být 2, avšak vzhledem k tomu, že tento znak se zde vyskytuje jen jednou a žádný jiný tomu není v celém textu podobný, je nepravděpodobné, že by to byla složenina dvou znaků. Nicméně to nelze vyloučit, protože čitelnost dokumentu není vysoká a také je nutno brát v potaz, že i pisatel mohl udělat chybu a znak přepsal, čímž by se snížila jeho čitelnost. V dokumentu se pak znak „a“ vyskytuje jako trojúhelník s tečkou uvnitř a i bez tečky. Bral jsem i možnost, že to mohou být dva různé znaky, ale překlad části textu (protože

je v italštině) dal jasně najevo, že je to tentýž znak. To samé se stejným výsledkem vyšlo i pro znak „+“. Nyní následuje přepis šifry a její dešifrovaná část.

```
4 r s 8   +   s r á 8   r   á +
m e n t o n e si t e   s i o
d 2 4 4   2   d g 5 +   c r   4 2 c r   s a +   a r
r a m m a r i c o   l e m a l e   n u o   u e
£ r   s   +   8 r á 8   r   & 2 d 8 g & r d
d e   n o t e si t e   p a r t i p e r
g c   á   r   d g s +   c   +   g s 5 ß r   g c   £ g á +
i l   si   e r i n o   l o   i n c h e   i l   d i   s i o
a £ g s   r   & 2 á   á   2 8 + ß 2   4 r 4 á +   g c
u d i n e   p a   s i   si a t o h a   m e m si o   i l
d r á 8   +   £ r c   c   r   & d + a g s 5 g r 5 2 8 +
r e si t o   d e l l e   p r o u i n c i e c a t o
c g 5 ß   r   £ g +   &   r d £ + s g   2 5 ß g 5 r
l i c h e   d i o   p e r d o n i   a c h i c e
á 8 2 8   2   c 2   5   2   l g + s r   r   4 r s 8 d r
si t a t a   l a c a   g i o n e   e   m e n t r e
g c   i8.   á r   d   g 8 g d 2 8 + 5 + s £ g 5 ß g
i l   da. di Corena   si e r   i t i r a t o c o n d i c h i
2 d 2 8   g + s r   £   g s + s a + c r d   á + d 8 g
a r a t   i o n e   d i n o n u o l e r   s i o r t i
```

d á + 8 8 + & d r 8 r á 8 + £ g s £ g á & + á g

s s
r i o t t o p r e t e si t o d i n d i i p o i i

8 g + s r d r á 8 2 2 c c 2 d m g 8 d g + £ r c

s
t i o n e r e i t a a l l a r si i t r i o d e l

4 + s £ + g c 3 + d 4 2 d s r & g a á g 5 a d

s
m o n d o i l f o r m a r n e p i u i i c u r

+ l g a á g 8 g + d r á 8 2 s á + 2 c c 2

o g i u si i t i o r e si t a n si o a l l a

5 a d 2 £ g iio r £ r l c g 2 c 8

iniciály
c u r a d i jména e d e g l i a l t

c
d g 5 2 & g £ r c c - d a 2 8 2 á & 2 l s

s
r i c a p i d e l l k r u a t a i p a g n

a + c 2 c 2 l r s 8 r s ß r 5 + 4 2 s £ 2 a 2

u o l a l a g e n t e n h e c o m a n d a u a

g c i8. á g & + 8 d 2 s s + á

da. di
i l Corena si i p o t r a n n o si

& r d 2 g s 2 a a r s g d r 4 g l c g + d g

p e r a i n a u u e n i r e m i g l i o r i

á a 5 5 r á á g 4 2 á á g 4 r 5 + s

si u c c e si si i m a si si i m e c o n

5 c a £ r 5 £ + + á g c 2 8 d r l a 2

c l u d e c d o o s i i l a t r e g u a
3 d 2 c 2 5 + d + s 2 £ g á & 2 l s 2 r
f r a l a c o r o n a d i s i p a g n a e
l c o + c 2 s £ r á 5 ß r s + s & 2 d
g l i o l a n d e s i c h e n o n p a r
2 3 3 2 8 8 + £ g á & r d 2 8 2
a f f a t t o d i s i p e r a t a

Na první pohled nemusejí slova dávat smysl, protože podle částečného překladu byly mezery tvořeny záměrně tak, aby skupina znaků netvořila vždy slovo. Tato šifra pracuje jen s několika písmeny, tudíž jsem mohl využít předchozí makro „`Frekvence`“, které se dá velmi lehce upravit k tomu, aby efektivně, nikoliv zdlouhavým způsobem, převedlo šifrové znaky, na znaky naší abecedy. Toto makro se jmenuje „`DekodovaniF`“.

```
Sub DekodovaniF()

Ax = 21
Bx = 23
Cx = 14

Dim kod As String

 For F = 1 To 25
  For j = 1 To 25
    For k = 1 To 30

          If Cells(Ax, j) = Cells(Cx, k) Then
          Cells(Bx, j) = Cells(Cx + 1, k)
          End If
Next k

Cells(Ax, j).HorizontalAlignment = xlCenter
Cells(Bx, j).Interior.Color = RGB(235, 160, 35)
Cells(Bx, j).HorizontalAlignment = xlCenter
Cells(Bx, j).Font.Bold = True
Cells(Bx, j).Font.Size = 10
Cells(Ax, j).Font.Size = 10

  Next j

   Ax = Ax + 4
   Bx = Bx + 4

 Next F
End Sub
```

Toto „DekodovaniF“ jsem, oproti předchozím, doplnil třetí proměnnou „Cx“. Je to z důvodu, že tato šifra je poměrně dlouhá a čím efektivnější bude kód, tím bude celý proces rychlejší a případné opravy jednodušší. V tomto kódu jsou využity tři cykly a to z důvodu toho, že je zároveň potřeba pracovat ve třech vrstvách. Proměnné „A-Cx“ představují vždy řádky v MS Excel, se kterými operují. V tomto případě je „Ax“ řádek v MS Excel, kde je samotná šifra (zašifrovaný text), „Bx“ řádek, kam má být dešifrovaný text přepsán a „Cx“ je první řádek dešifrovací tabulky, kde jsou obsaženy znaky šifrové abecedy. Celý proces převodu je jednodušší, než u předchozích maker. V tomto případě šel postup vyřešit jednoduchou podmínkou „If“, která se ptá, jestli se obsah buňky v řádku se šifrou `Cells(Ax, j)`, rovná se znakem šifrové abecedy v dešifrovací tabulce `Cells(Cx, k)`. Zde je vidět, proč byl nutný třetí cyklus. Pokud by totiž nebyl, hodnoty posunu „j“ by byly stejné, jak pro znak v šifrovaném textu, tak

i pro řádek v dešifrovací tabulce. Třetí cyklus zajistí, že pro souřadnice `(Ax, j)` bude otestována celá řada `(Cx, k)`, kde „`Cx`“ je zvoleno a „`k`“ počet opakování jasně daný. V tomto případě se tedy otestuje znak po znaku, dokud není nalezena shoda. Pokud by se tak nestalo (například mezery), potom cyklus pokračuje s další hodnotou v `(Ax, j)`, kde oproti předchozímu kroku je už `(Ax, j+1)`. Jestliže je shoda nalezena, pak se do `Cells(Bx, j)` nahraje hodnota `Cells(Cx + 1, k)`. V tomto je toto řešení tak jednoduché, protože když se najde shoda, stačí „skočit“ o řádek níže, kde se nachází správný dešifrovací znak (v našem případě písmena). Následné vzhled upravující funkce jsou naprosto stejné jako v předchozích makrech.

```
Sub Frekvence ()

Ax = 21
Bx = 125
Cx = 14

For k = 1 To 30
     Cells(Bx, k) = 0
Next k

 For F = 1 To 25
     For j = 1 To 25
          For k = 1 To 30
               If Cells(Ax, j) = Cells(Cx, k) Then
               Cells(Bx, k) = Cells(Bx, k) + 1
               End If
          Next k
     Next j

     Ax = Ax + 4

  Next F

End Sub
```

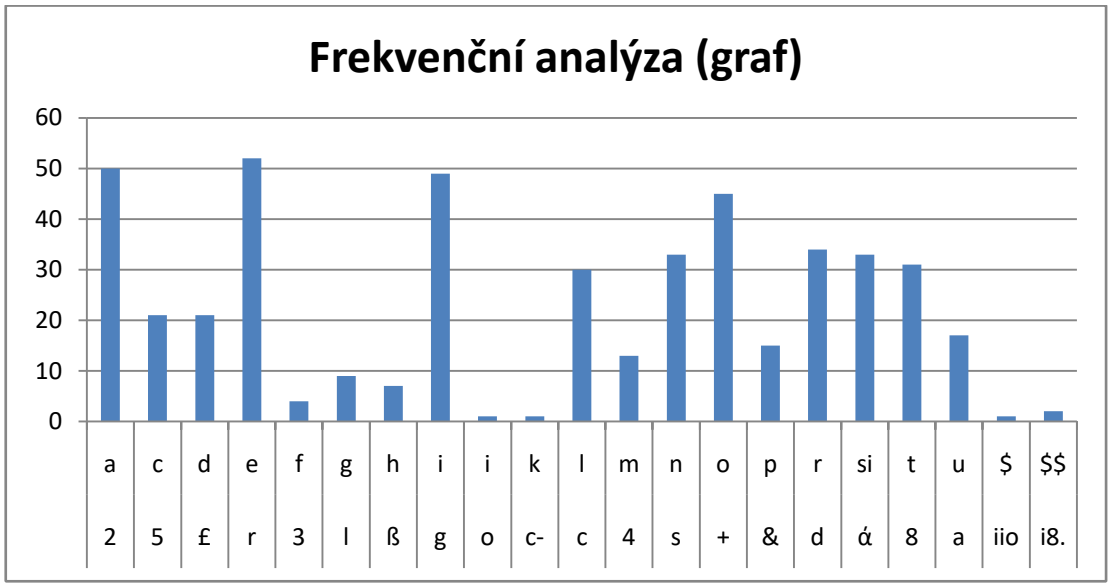
Makro „Frekvence“ zůstalo naprosto totožné, jako v předchozí šifře. Jediná změna je ta, že v tomto makru figuruje proměnná „Cx“. První proměnná „Ax“ udává první řádek zašifrovaného textu, „Bx“ kam se mají připisovat hodnoty a „Cx“ s čím se mají čtené hodnoty porovnávat. Jak jsem již zmínil v předešlém případě, makro hledá shodu a pokud ji nalezne, tak na danou pozici přičte číslo 1. Díky tomuto makru, lze sestavit tabulku s podmíněným formátováním, ze které jsou patrná nejčastější písmena a i znaky.

Tabulka č. 6 – Frekvenční analýza

2	**5**	**£**	**r**	**3**	**l**	**ß**	**g**	**o**	**c-**	**c**	**4**	**s**	**+**	**&**	**d**	**á**	**8**	**a**	**iio**	**i8.**
a	c	d	e	f	g	h	i	i	k	l	m	n	o	p	r	si	t	u	$	$$
50	**21**	**21**	**52**	**4**	**9**	**7**	**49**	**1**	**1**	**30**	**13**	**33**	**45**	**15**	**34**	**33**	**31**	**17**	**1**	**2**

$ iniciály jména
$$ da. di Corena

Díky získaným datům v této tabulce jsem mohl sestavit graf frekvenční analýzy, na kterém, podobně jako v tabulce, je vidět spektrum nejpoužívanějších znaků v konkrétním jazyce (zde konkrétně v italštině) pomocí podmíněného formátování. Podle výsledkům těchto analýz je vidět rozdíl mezi francouzštinou a italštinou, ve smyslu používání určitých samohlásek. Zde je pro lepší přehlednost graf.



Graf č. 3 – Frekvenční analýza

4.4 Šifra v dokumentu 25106

Tabulka č. 7 – Dešifrovací tabulka

X	0	1	2	3	4	5	6	7	8	9
0										
1	?	c	?		d		a	a		e
2	?	–	g	?	h		e	?		
3		l/del	l	?	m	?	i	i		m
4	p	q	n		r		o	o	?	?
5			s	?		due	u/v	u/v		
6	t		I.	–		?				
7	–		–							
8							?			
9										

Tuto šifru jsem zvolil jako poslední, jelikož její luštění bylo nejobtížnější. Dokument k této šifře byl pravděpodobně psán ve spěchu, tudíž sám o sobě je špatně čitelný. Další problém u tohoto dokumentu je ten, že jak je vidět z tabulky, některé znaky znamenají více možnosti, jedná se tedy o homofonní šifru. Jak je patrné z tabulky, mnoho znaků nese otazník. Je to protože u nich nebylo možné zjistit s přesností co je to za znak. I tato šifra je podobně jako předchozí „čtvercová“ šifra založena na principu Polybiova čtverce. Nyní následuje přepis šifry s dešifrovaným textem.

5 2 6 3 4 6
5 6 6 44 17 34 26 42 0 26 37 31 4 6 14 27 31 60 44 12 0 17

u/ l/d l/d
v e r a m e n t e i el m o d ? el t r ? t a

4 1 3 2 4 4
4 4 26 31 62 55 14 6 31 46 44 6 2 26 60 17 42 16 60 7 17

l/d du l/d
r d e el I. e d i el o r e n e t a n a t o a

4 4 1 1 4 4
8 1 57 17 42 60 47 7 34 26 40 6 4 56 42 24 36 52 60 7 44

u/ u/
? q v a n t o a m e p a r v n h i s t o r

3 1 2 4 4 4
6 6 14 16 31 27 21 7 44 52 46 0 4 16 56 42 31 36 10 4 4

l/d u/ l/d
i a d a el ? – ? r s o p r a v n el i ? r

4 1 4 4 1
4 7 9 16 34 26 40 17 4 17 42 11 6 4 17 22 52 46 40 44 6 31 17

l/d
o e a m e p a r a n c o r a g s o p r a el a

5 5 4 3 5 4
2 6 16 40 26 44 52 6 42 16 56 7 2 36 16 14 26 20 17 4 4

s u/ v a p e r s o n a u/ v i s i a d e ? a r

4 4 1 2 4
0 6 11 47 20 46 42 4 17 21 34 6 2 60 46

p o c o ? o n d a – m e n t o

5 1 4
2 1 44 36 56 46 42 6 14 16

s c r i u/ v o n o d a

3 1 2 1 6 1 4
2 6 44 39 16 60 26 2 36 32 39 6 0 53 20 26 31 60 14 6 46 21 2 36

l a r m a t e g i l m a t ? ? e l/d e l t d a o – n i

2 3 2 4 1 4 5
1 6 46 44 42 46 34 6 42 46 52 6 4 86 52 20 16 60 36 6 42 26 6 52

– i o r n o m e n o s o d ? s ? a t i o n e u/ v s

1 2 4 3 1 5 1
9 2 22 26 22 31 36 6 20 36 60 6 6 31 36 52 26 31 36 2 46 31 9 16

e g g e g l/d e l i o ? i t i a l/d e l i s e l/d e l i s o l/d e l e a

6 3 4 4 2 5
0 6 33 31 60 36 40 6 44 60 16 2 6 16 34 46 44 26 22 6 44 36 2 40

t i ? l/d e l t i p o r t a n o a m o r e g e r i s p

2 6 5 4 4 3 4
6 0 46 31 16 14 36 2 56 42 36 6 2 26 35 36 11 16 40 6 52 16 2 14

e t o l/d e l a d i s u/ v n i o n e ? i c a p i s a n d

1 5 4 2 3 2 3
6 6 16 52 26 34 40 4 26 34 16 2 6 46 44 34 26 42 60 6 16 56 4 26

a u/ v a s e m p r e m a g i o r m e n t e a u/ v m e

4	6						4				1	3							1			4	
2	0	16	49	14	46	36	2	52	46	34	6	6	46	23	56	26	14	46	6	31	60	4	46

															u/					l/d			
n	**t**	**a**	**?**	**d**	**o**	**i**	**n**	**s**	**o**	**m**	**a**	**i**	**o**	**?**	**v**	**e**	**d**	**o**	**a**	**el**	**t**	**r**	**o**
4	2						2				3	6							6			1	
4	6	34	26	14	36	46	2	36	31	44	6	0	46	44	42	46	14	36	5	31	16	2	31

									l/d											l/d			l/d
r	**e**	**m**	**e**	**d**	**i**	**o**	**g**	**i**	**el**	**r**	**i**	**t**	**o**	**r**	**n**	**o**	**d**	**i**	**?**	**el**	**a**	**?**	**el**
2	2						4				6	1							5			3	
6	6	14	26	52	14	26	4	16	60	16	0	6	42	60	46	14	16	60	6	60	36	6	11

																		u/				
e	**e**	**d**	**e**	**s**	**d**	**e**	**r**	**a**	**t**	**a**	**t**	**a**	**n**	**t**	**o**	**d**	**a**	**t**	**v**	**t**	**i**	**i**	**c**
1	4						1				4	3							4			1	
6	0	36	12	42	60	46	4	16	36	52	6	5	14	16	60	36	19	40	4	36	42	1	36

a	**p**	**i**	**?**	**n**	**t**	**o**	**d**	**a**	**i**	**s**	**o**	**?**	**d**	**a**	**t**	**i**	**e**	**p**	**r**	**i**	**n**	**c**	**i**
4	1						2				2	1							3			4	
0	6	31	34	26	42	60	6	14	16	32	6	1	16	56	16	31	26	44	6	16	11	6	34

		l/d											u/		l/d								
p	**a**	**el**	**m**	**e**	**n**	**t**	**e**	**d**	**a**	**l**	**e**	**c**	**a**	**v**	**a**	**el**	**e**	**r**	**i**	**a**	**c**	**o**	**m**
2	1						4				1	7							2			3	
6	6	42	11	46	19	56	2	16	21	44	6	2	40	16	44	60	26	14	3	31	16	6	11

						u/													l/d			
e	**a**	**n**	**c**	**o**	**e**	**v**	**n**	**a**	**–**	**r**	**a**	**–**	**p**	**a**	**r**	**t**	**e**	**d**	**?**	**el**	**a**	**i**	**c**
4	4						4				1	5							1			5	
6	2	52	26	31	21	26	4	36	19	11	6	6	16	31	21	26	44	36	4	26	31	2	16

				l/d							u/		l/d							l/d		
o	**n**	**s**	**e**	**el**	**–**	**e**	**r**	**i**	**e**	**c**	**a**	**v**	**a**	**el**	**–**	**e**	**r**	**i**	**d**	**e**	**el**	**s**	**a**
1	4						2				3	3							5			1	
1	6	44	60	26	16	31	0	56	31	60	6	4	46	44	16	42	19	26	2	36	31	6	11

						l/d		u/	l/d												l/d		
c	**o**	**r**	**t**	**e**	**a**	**el**	**?**	**v**	**el**	**t**	**i**	**m**	**o**	**r**	**a**	**n**	**e**	**e**	**s**	**i**	**el**	**a**	**c**
1	5						1				1	4							2			5	
6	6	16	31	26	44	36	6	11	44	36	4	6	14	56	26	56	46	31	6	56	36	6	16

	u/		l/d										u/		u/		l/d		u/		u/	
a	**v**	**a**	**el**	**e**	**r**	**i**	**a**	**c**	**r**	**i**	**d**	**o**	**d**	**v**	**e**	**v**	**o**	**el**	**e**	**v**	**i**	**v**	**a**
4	3						3				3	1							3				
0	6	11	46	31	46	34	6	42	36	40	6	1	63	46	31	46	39	70	6	42	36		

Vzhledem k šířce řádků v dokumentu, ze kterého jsem prováděl přepis, jsou některé číslice pod sebou, avšak vždy se jedná o dvojici cifer. Na toto dešifrování jsem použil makro „Dekodovani“, které jsem použil i u předchozí čtvercové šifry. Jediný rozdíl je ten, že vstupní hodnota „a“ která uvádí řádek je jiná, stejně tak hodnota „B“, která uvádí řádek, kam se provede přepis. Tato šifra, se jako jediná, nepodařila zcela rozluštit. Pro zajímavost jsem vymyslel makro, které na základě dešifrovaného textu umí zjistit, jaká je procentuální úspěšnost rozluštění této šifry.

```
Sub procento()

a = 17
For x = 1 To 25
     For i = 1 To 35

          If Cells(a, i) = "?" Then
               Cells(136, 41) = Cells(136, 41) + 1
               ElseIf Cells(a, i) > 0 Then
               Cells(136, 40) = Cells(136, 40) + 1
          End If

     Next i

     a = a + 4
Next x

  Cells(137, 40) = (((Cells(136, 41) / Cells(136, 40)) *
100) * (-1)) + 100

End Sub
```

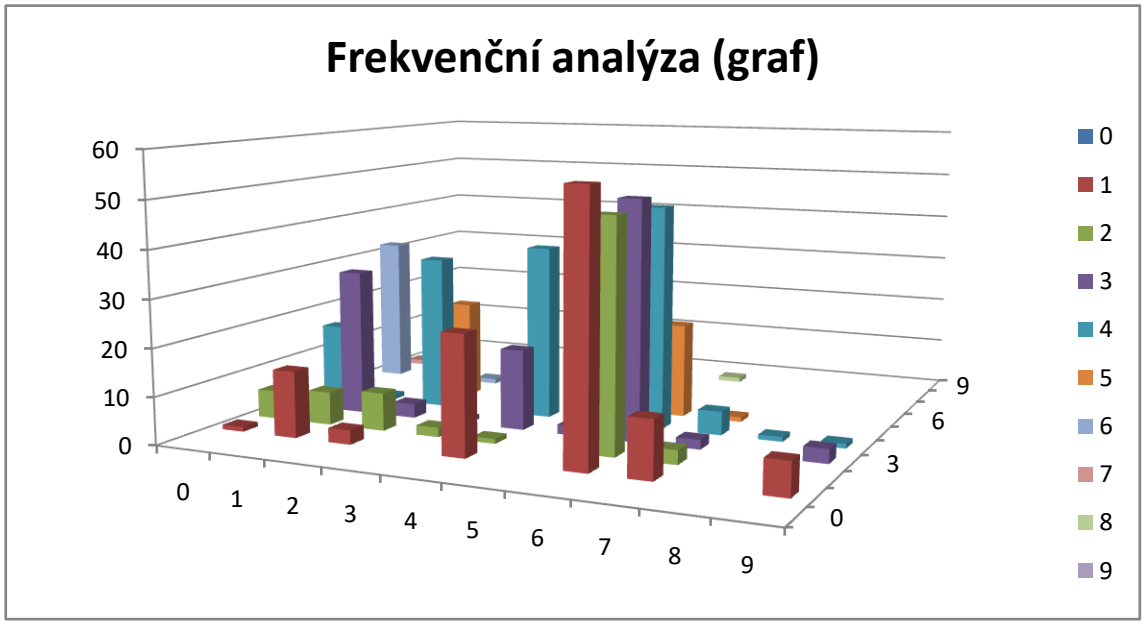
Toto jednoduché makro pracuje s dvěma cykly, protože jeho základ je z makra „Dekodovani“. Jediné co se v cyklech děje je to, že dvě podmínky hledají zadané hodnoty. Ta první z nich znak „?“ a druhá hodnoty větší než 0, aby se nezapisovaly mezery. Hodnoty se uloží do přesně daných buněk a po skončení cyklů se do třetí buňky vypočítá procentuální úspěšnost. Po dokončení tohoto makra se v buňce objeví krásné číslo a to 95,41%.

Dále makrem „frekvence“, které je stejné s předchozím makrem „frekvence“ v čtvercové šifře, jsem získal tabulku dat s četností znaků, na kterou jsem použil opět podmíněné formátování.

Tabulka č. 8 – Frekvenční analýza

X	0	1	2	3	4	5	6	7	8	9
0										
1	1	14	3		25		55	12		7
2	6	7	8	2	1		48	3		
3		31	3	1	17	2	50	2		3
4	16	1	33		37		47	5	1	1
5			21	1		1	20	1		
6	32		1	1		1				
7	1		1							
8							1			
9										

Na této tabulce je dobré si povšimnout hodnot 1. Tyto hodnoty jsou totiž nerozluštěné otazníky, které se v textu objevují pouze jednou, a nebylo možné je rozluštit. Avšak ne všechny otazníky jsou v textu jednou, některé i vícekrát, ale problém s jejich vyluštěním je stejný. Naproti tomu zelená čísla ve sloupci 6 nám jasně ukazují, že se jedná o samohlásky. Pro lepší vizuální přehlednost jsem podle této tabulky vytvořil graf, na kterém je lépe vidět rozdíl v používání různých písmen.



Graf č. 4 – Frekvenční analýza

Závěr

Cílem práce bylo podrobit historické šifry analýze, a tím získat alespoň částečnou dešifrovací tabulku, a ze získaných dat provést frekvenční analýzu, která by mohla doplnit dešifrovací tabulku, což by mohlo vést k úplnému rozluštění šifry. Tato práce byla rozdělena do čtyř kapitol, protože se každá tematicky liší.

V první kapitole jsem shrnul základní poznatky o kryptologii, kde jsem následoval se stručným vývojem historických šifer, které jsem obohatil o obrázky a doplňující tabulky, protože si myslím, že vidět danou problematiku i vizuálně vede k lepšímu porozumění.

V kapitole druhé, kde jsem zmiňoval vývoj programu MS Excel, jsem se více zaměřil na využití jazyka VBA v mé práci, kde jsem popsal konkrétní syntaktické konstrukce, které jsem využil při psaní maker.

Třetí kapitolu jsem věnoval především Piccolominiům, avšak velice stručně. Samotnému rodu jsem nemohl věnovat více prostoru, jelikož historie tohoto rodu není tématem této práce. Důležitější mi proto přišlo napsat samotnou podkapitolu o Otaviovi Piccolomini, protože je pravděpodobně příjemce všech šifer, které jsou obsažené v této práci, tedy všechny v práci uvedené šifry znal a používal. K této kapitole jsem připojil ještě popis své návštěvy SOA Zámrsk, protože to pro mne bylo opravdu velmi přínosné a v budoucnu bych se tam rád vrátil a našel ještě nějaké nerozluštěné šifry.

V poslední kapitole, která je de facto praktickou částí práce, bylo cílem pokusit se dané texty dešifrovat. Na základě analýzy textů bylo možno zjistit několik písmen a s jejich pomocí a s použitím metody předpokládaných slov postupně přidávat další písmena. Pro statistické ověření správnosti luštění bylo možno provést frekvenční analýzu, která navíc posloužila i ke zjištění jazyka otevřeného textu. Po úvodním částečném dešifrování bylo možné u většiny šifer postupnými kroky dosáhnout kompletního dešifrování.

Podle mého názoru se cíle práce podařilo splnit a dokonce překročit. První tři šifry se podařilo rozluštit s úspěšností 100%. Poslední šifra, jako jediná, se podařila rozluštit na 95,4% a to především díky nečitelnosti znaků v původním textu. Díky provedené počítačové analýze a následně i frekvenční analýze (která potvrdila správnost luštění) jsem byl schopen říci, jaký jazyk otevřeného textu byl šifrován. Tato skutečnost vyplynula samozřejmě i z dešifrovaného textu, po spuštění dešifrovacího makra.

Osobně se domnívám, že tato práce byla přínosná a rád bych chtěl na tuto prací navázat, jen v mnohem širším a komplexnějším měřítku.

Seznam použité literatury

Literatura

1. BURDA, Karel. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM, 2015, 108 s. ISBN 978-80-7204-925-7.
2. ČERNÝ, Jaroslav. *Excel 2000-2007: záznam, úprava a programování maker*. 2., aktualiz. vyd. Praha: Grada, 2007, 183 s. Průvodce. ISBN 978-80-247-2305-1.
3. JANEČEK, Jiří. *Gentlemani (ne)čtou cizí dopisy*. Brno: BOOKS, 1998, 175 s., 8 s. il. příl. Bonus A. ISBN 80-85914-90-5.
4. JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry*. Praha: Naše vojsko, 1994, 183 s. Mozaika. ISBN 80-206-0462-6.
5. JANEČEK, Jiří. *Rozluštěná tajemství: luštitelé, dešifranti, kódy a odhalení*. Praha: XYZ, 2006, 268 s. ISBN 80-86864-54-5.
6. LAURENČÍK, Marek a Michal BUREŠ. *Programování v Excelu 2007 & 2010: záznam, úprava a programování maker*. Praha: Grada, 2011, 190 s. Průvodce. ISBN 978-80-247-3448-4.
7. LUNDE, Paul. *Tajemství kódů: [nahlédněte do světa skrytých poselství: ilustrovaný průvodce znameními, symboly, šiframi a tajnými jazyky]*. Přeložil Erika STAŘECKÁ. Praha: Svojtka & Co., 2013, 279 s. ISBN 978-80-256-0978-1.
8. SINGH, Simon. *Code book: the science of secrecy from ancient Egypt to quantum cryptography*. New York: Anchor Books, 1999. ISBN 978-0-385-49532-5.
9. 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, 382 s. Aliter. ISBN 978-80-7363-268-7.
10. VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.
11. WACHSMANNOVÁ, Viktorie a Jarmila BLAŽKOVÁ. *Náchod: státní zámek a okolí*. 2. přeprac. a rozš. vyd. Praha: Sportovní a turistické nakladatelství, 1958, 42 s. Publikace Státní památkové správy.

12. WEBER, Monika a Melanie BREDEN. *Excel VBA: velká kniha řešení*. Brno: Computer Press, 2007, 867 s. Programování. ISBN 978-80-251-1453-7.

Internetové zdroje

1. *Albrecht von Wallenstein* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Albrecht_von_Wallenstein>
2. *Microsoft Excel* [online, cit. 24. 4. 2017], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Microsoft_Excel>
3. *Ottavio Piccolomini* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Ottavio_Piccolomini>
4. *Piccolomini* [online, cit. 21. 4. 2017], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Piccolomini>

Tabulky a grafy

Tabulky

Grafy

Seznam použitých obrázků

1. Skytala
2. Polybius
3. Gaius Julius Caesar
4. Gaius Octavianus (Augustus)
5. Leon Battista Alberti
6. Johannes Trittheim
7. Hieronymus Cordanus
8. Blaise Vigenére
9. Armand-Jean du Plessis Richelieu
10. Francis Bacon
11. Enigma
12. Rodový erb Piccolominiů
13. Erb Otavia Piccolomini
14. Otavio Piccolomini

Zdroje použitých obrázků

1. http://www.romeandart.eu/images/news/cifrario-4.jpg
2. https://upload.wikimedia.org/wikipedia/commons/a/a7/Polybios_head.JPG
3. https://upload.wikimedia.org/wikipedia/commons/thumb/4/47/Caesar.jpg/189px-Caesar.jpg
4. https://upload.wikimedia.org/wikipedia/commons/7/7b/Caesar-augustus1.jpg
5. https://upload.wikimedia.org/wikipedia/commons/8/84/Leon_Battista_Alberti2.jpg
6. https://upload.wikimedia.org/wikipedia/commons/f/f2/Trithemius.jpg
7. https://upload.wikimedia.org/wikipedia/commons/thumb/2/2f/Girolamo_Cardano._Stipple_engraving_by_R._Cooper._Wellcome_V0001004.jpg/800px-Girolamo_Cardano._Stipple_engraving_by_R._Cooper._Wellcome_V0001004.jpg
8. https://upload.wikimedia.org/wikipedia/commons/1/1a/Vigenere.jpg
9. https://upload.wikimedia.org/wikipedia/commons/b/b4/Armand%2C_Jean_du_Plessis.jpg

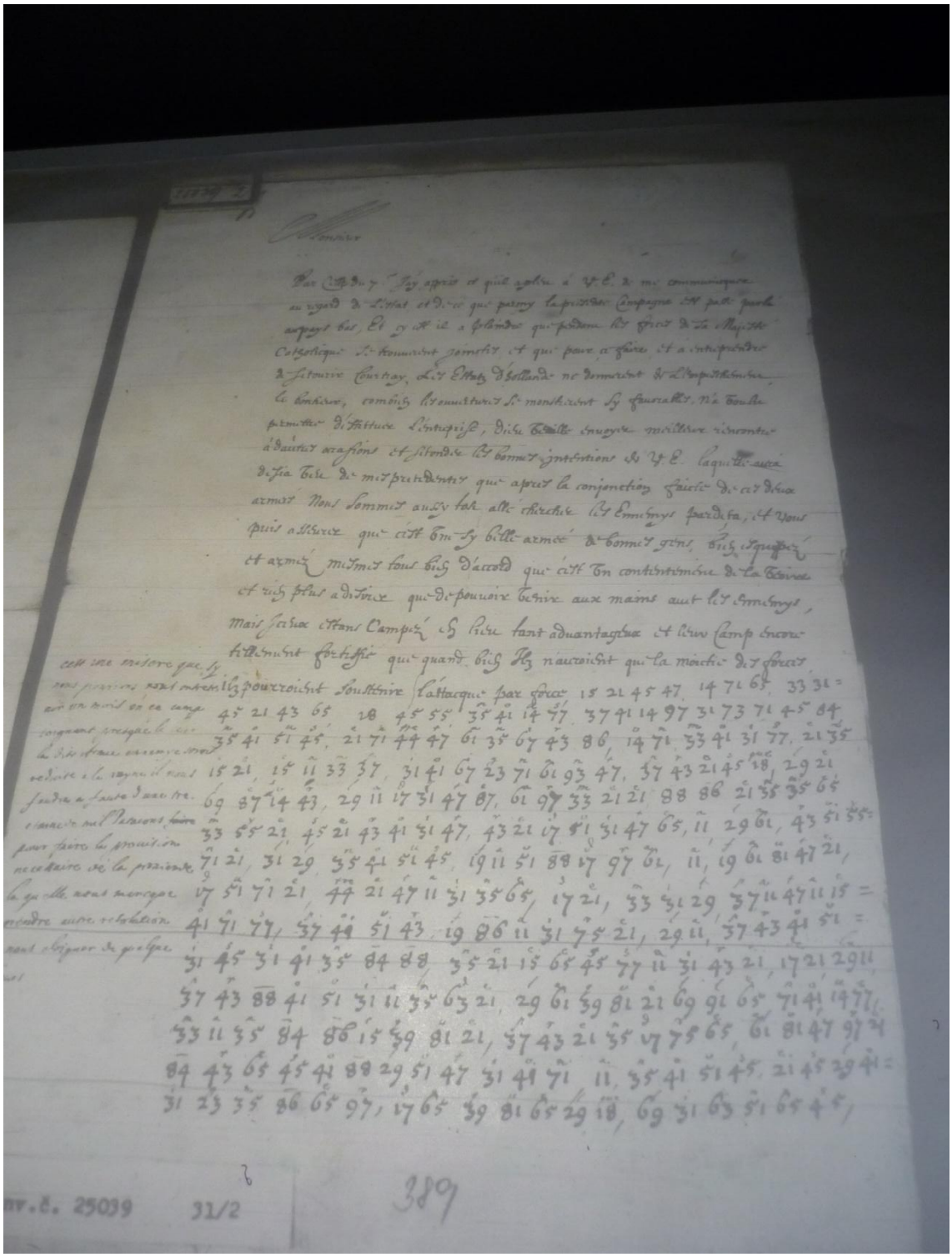
10. https://upload.wikimedia.org/wikipedia/commons/a/a7/Pourbus_Francis_Bacon.jpg
11. https://upload.wikimedia.org/wikipedia/commons/thumb/2/27/Enigma-plugboard.jpg/640px-Enigma-plugboard.jpg
12. https://upload.wikimedia.org/wikipedia/commons/thumb/5/55/Coat_of_arms_of_the_House_of_Piccolomini.svg/220px-Coat_of_arms_of_the_House_of_Piccolomini.svg.png
13. https://upload.wikimedia.org/wikipedia/commons/thumb/0/07/Piccolomini_Pieri_d%27Aragona.png/220px-Piccolomini_Pieri_d%27Aragona.png
14. https://upload.wikimedia.org/wikipedia/commons/thumb/8/81/Anselmus-van-Hulle-Hommes-illustres_MG_0469.tif/lossy-page1-800px-Anselmus-van-Hulle-Hommes-illustres_MG_0469.tif.jpg

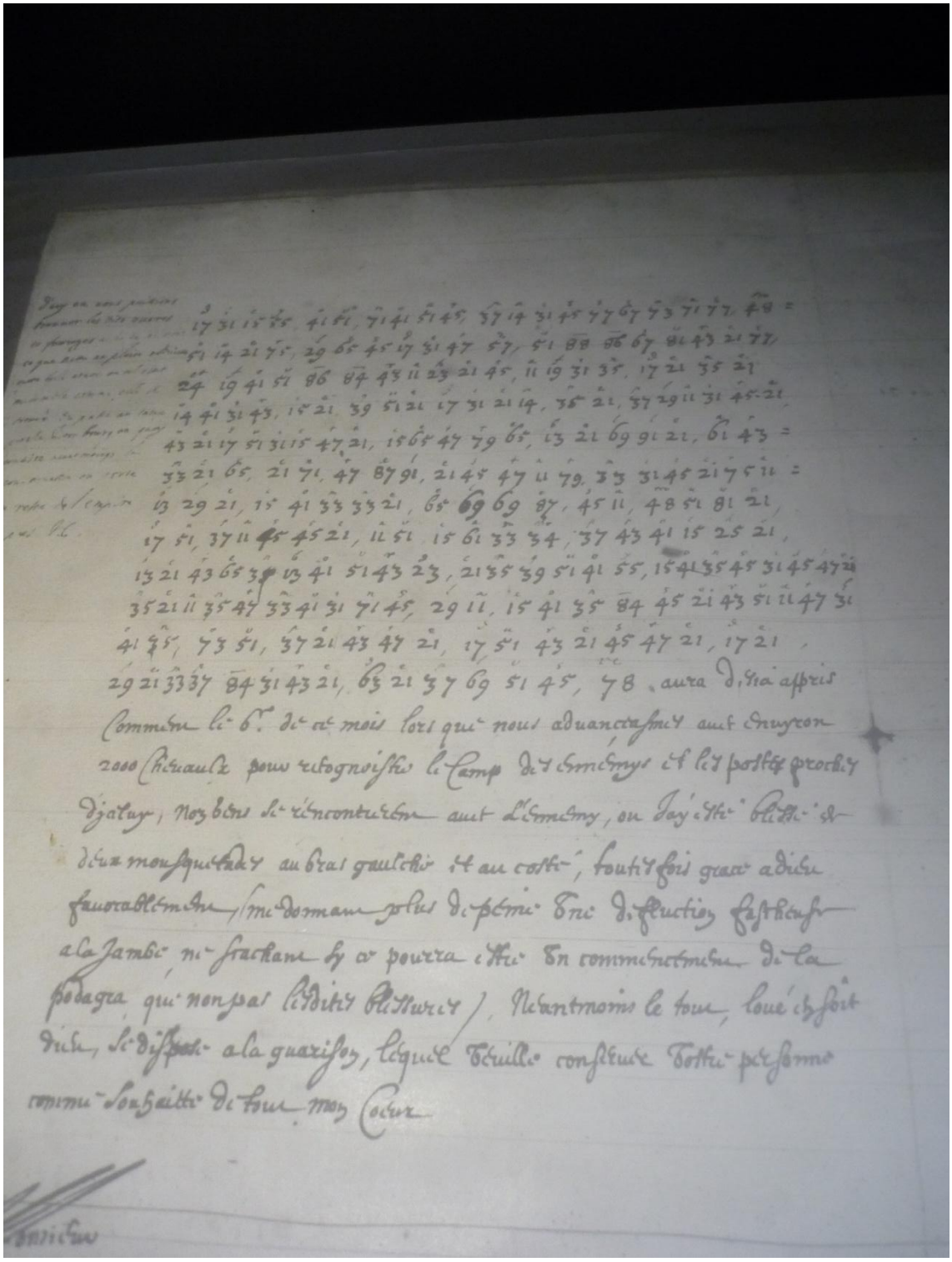
Seznam příloh

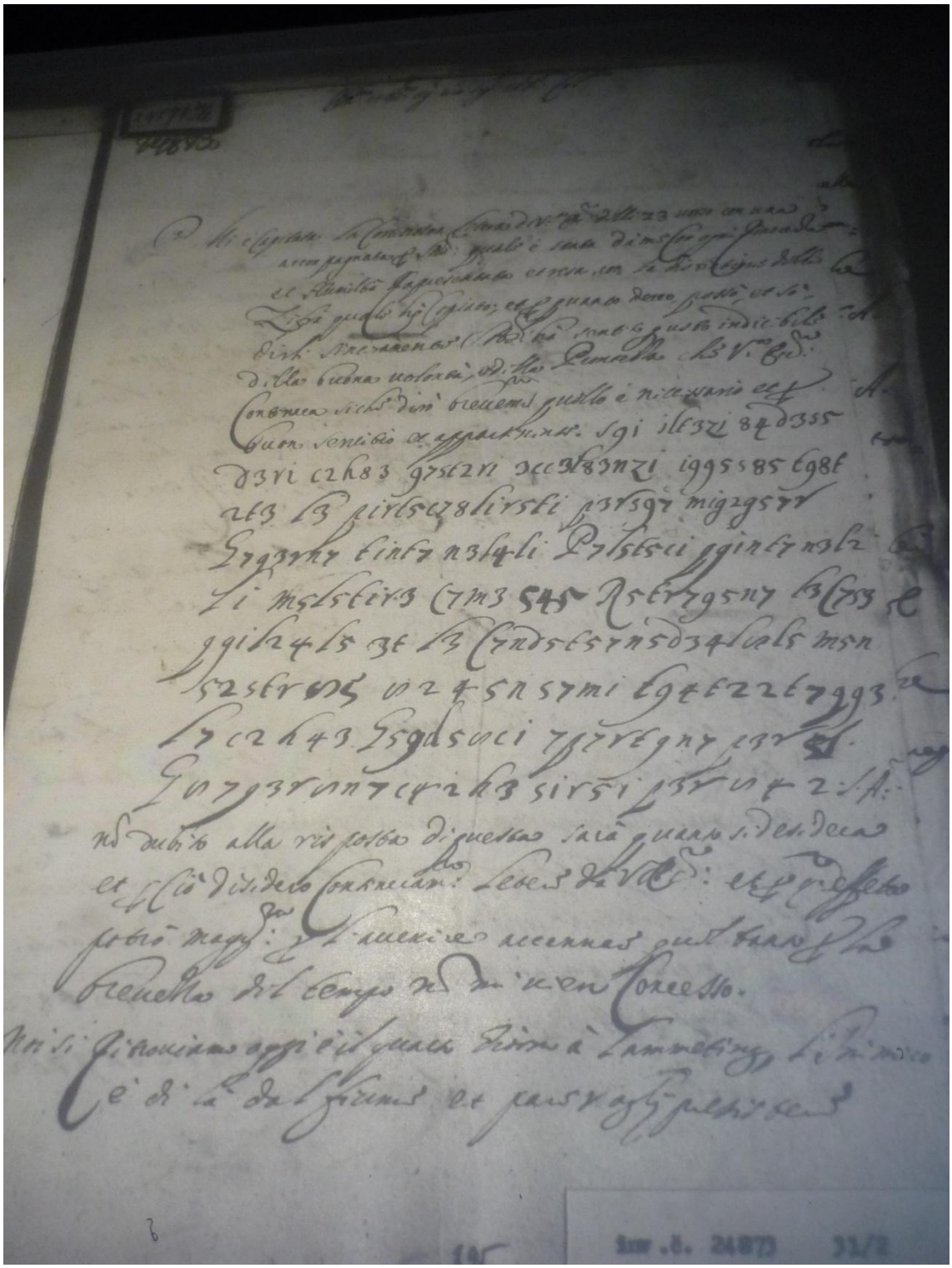
A. Fotokopie šifrových textů, které byly v práci dešifrovány

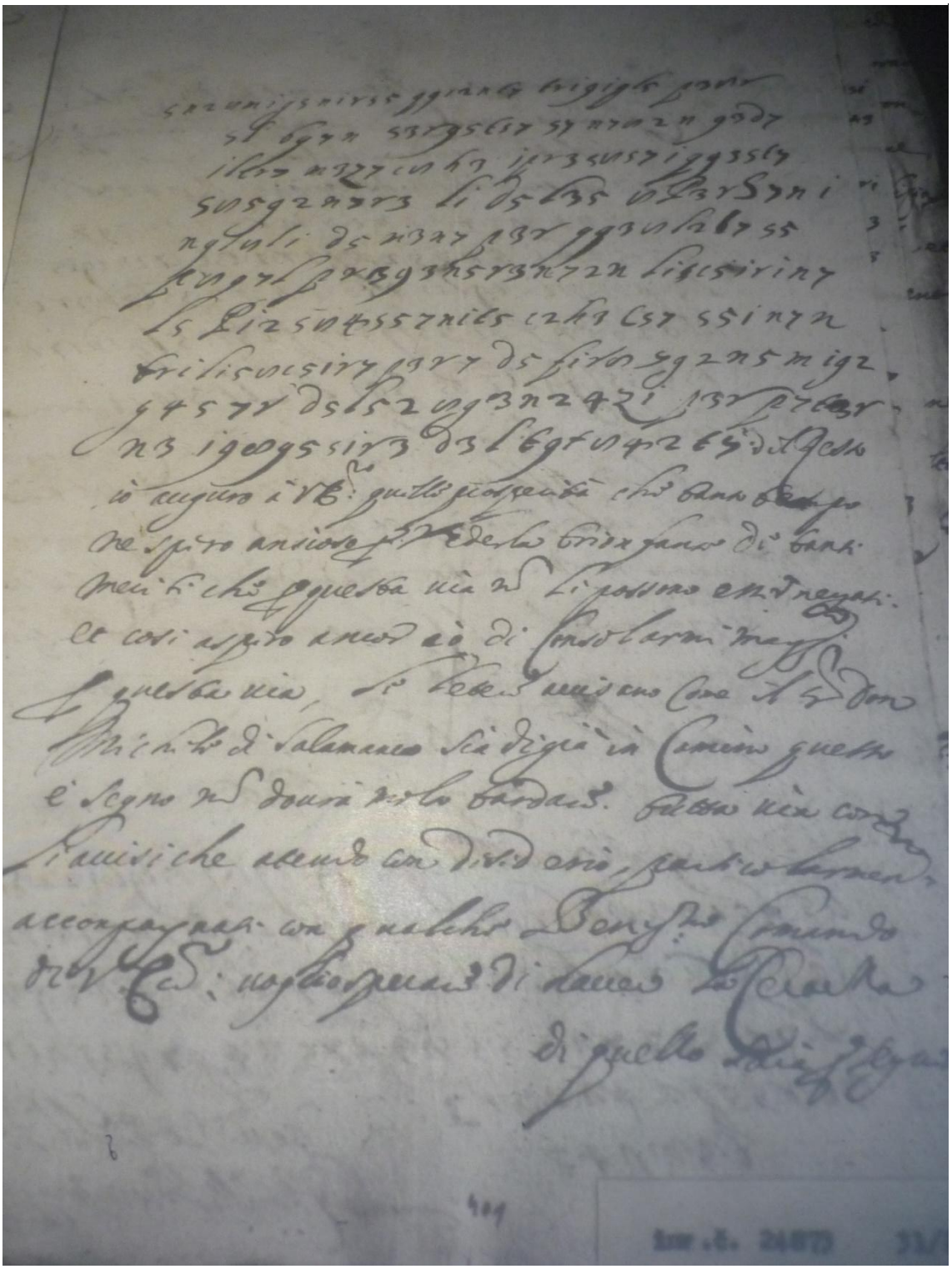
(tyto fotokopie jsou přiloženy v tištěné podobě i elektronicky)

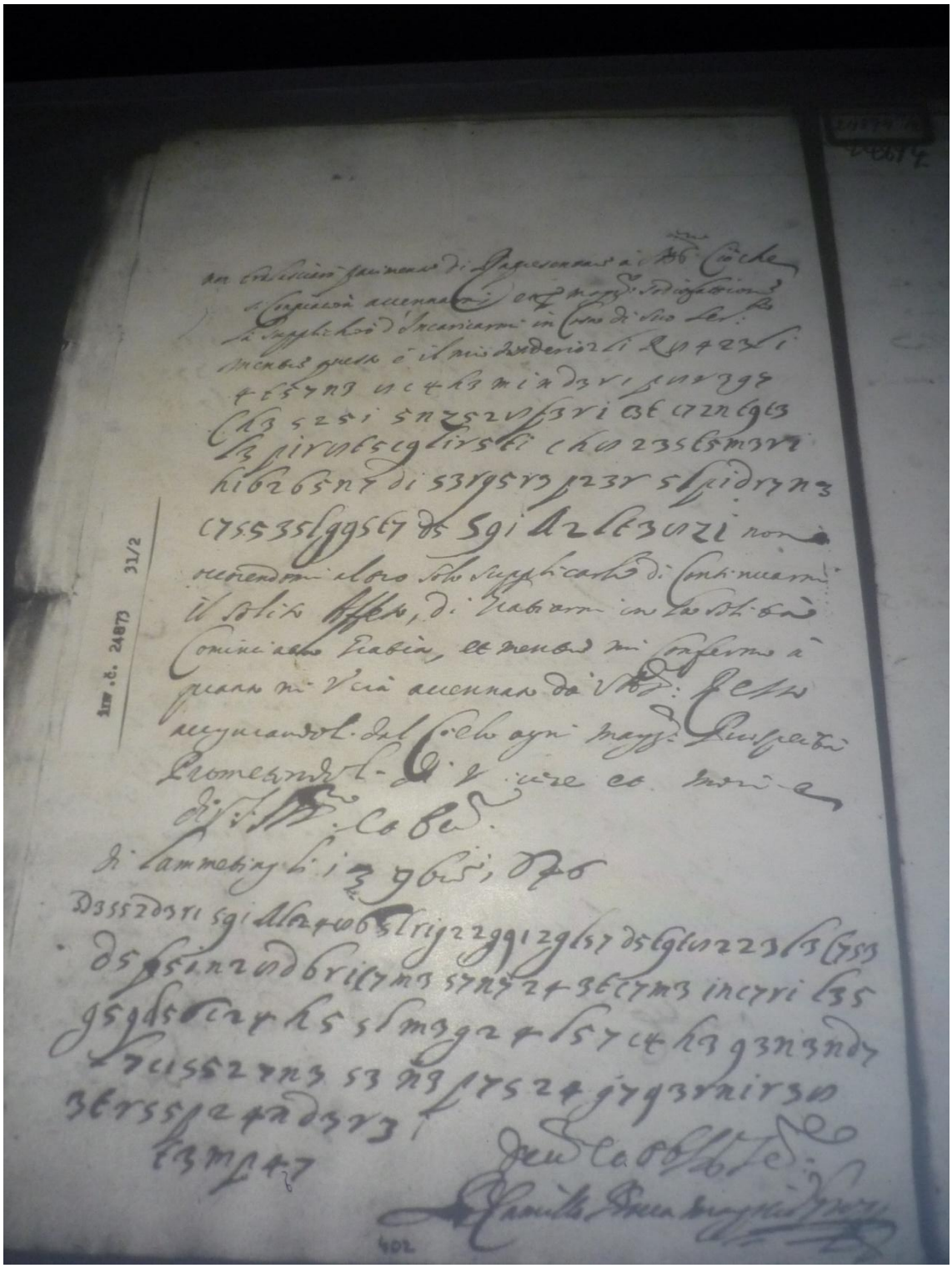
A01	Dokument s inventárním číslem 25039
A02	Dokument s inventárním číslem 25039_1
A03	Dokument s inventárním číslem 24873
A04	Dokument s inventárním číslem 24873_1
A05	Dokument s inventárním číslem 24873_2
A06	Dokument s inventárním číslem 24790
A07	Dokument s inventárním číslem 25106
A08	Dokument s inventárním číslem 25106_1
A09	Dokument s inventárním číslem 25106_2
A10	Dokument s inventárním číslem 25106_3

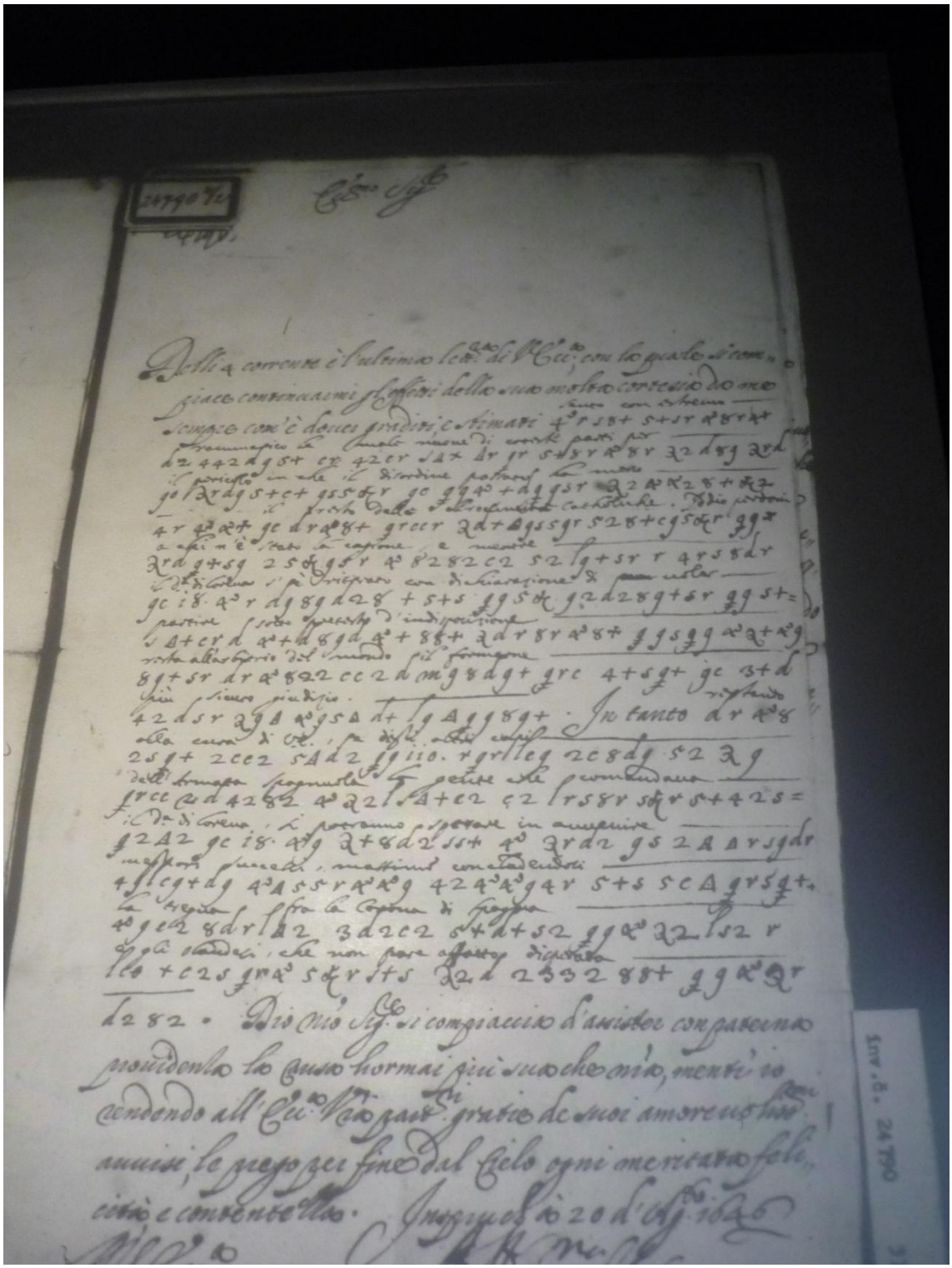


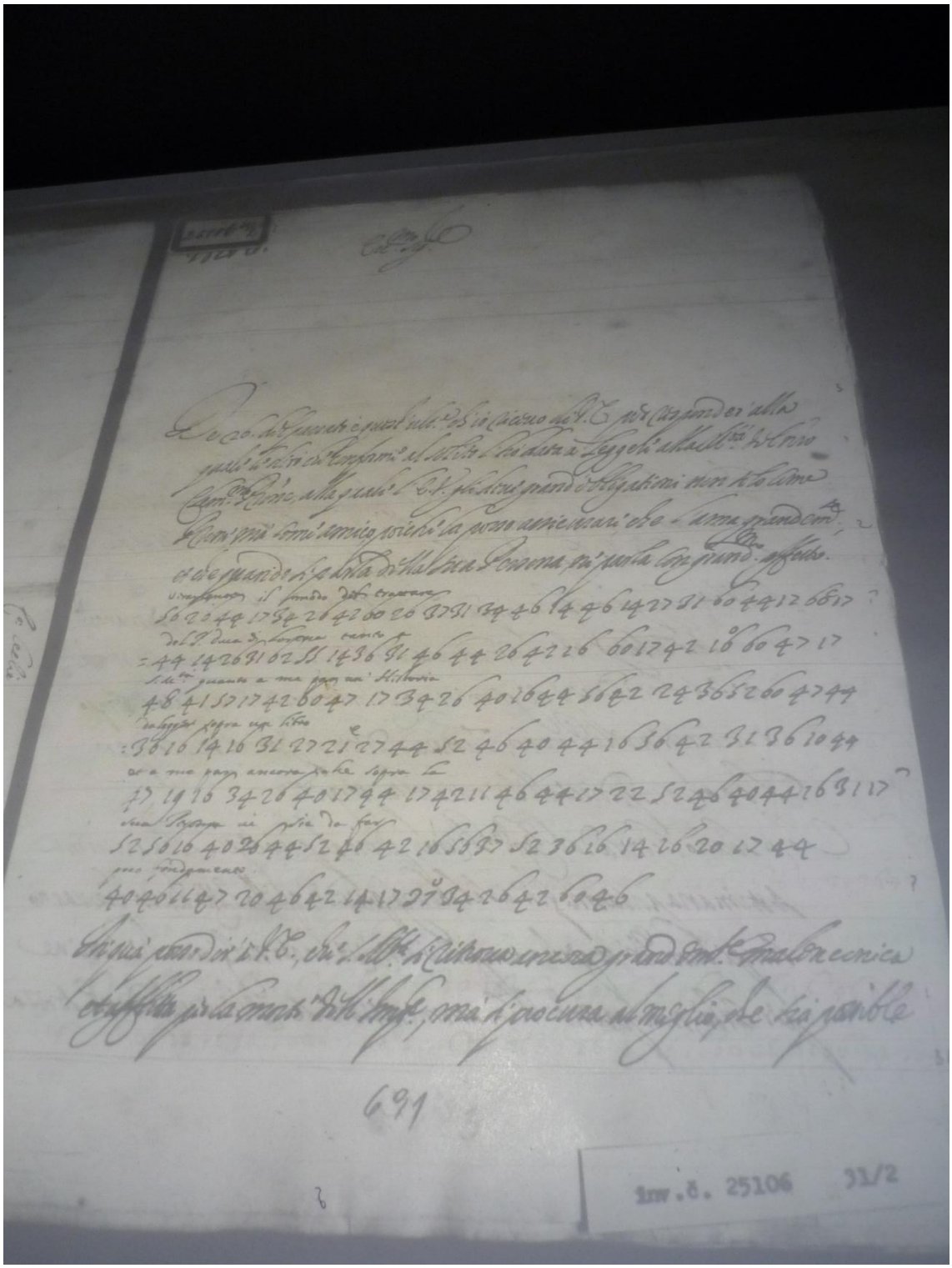


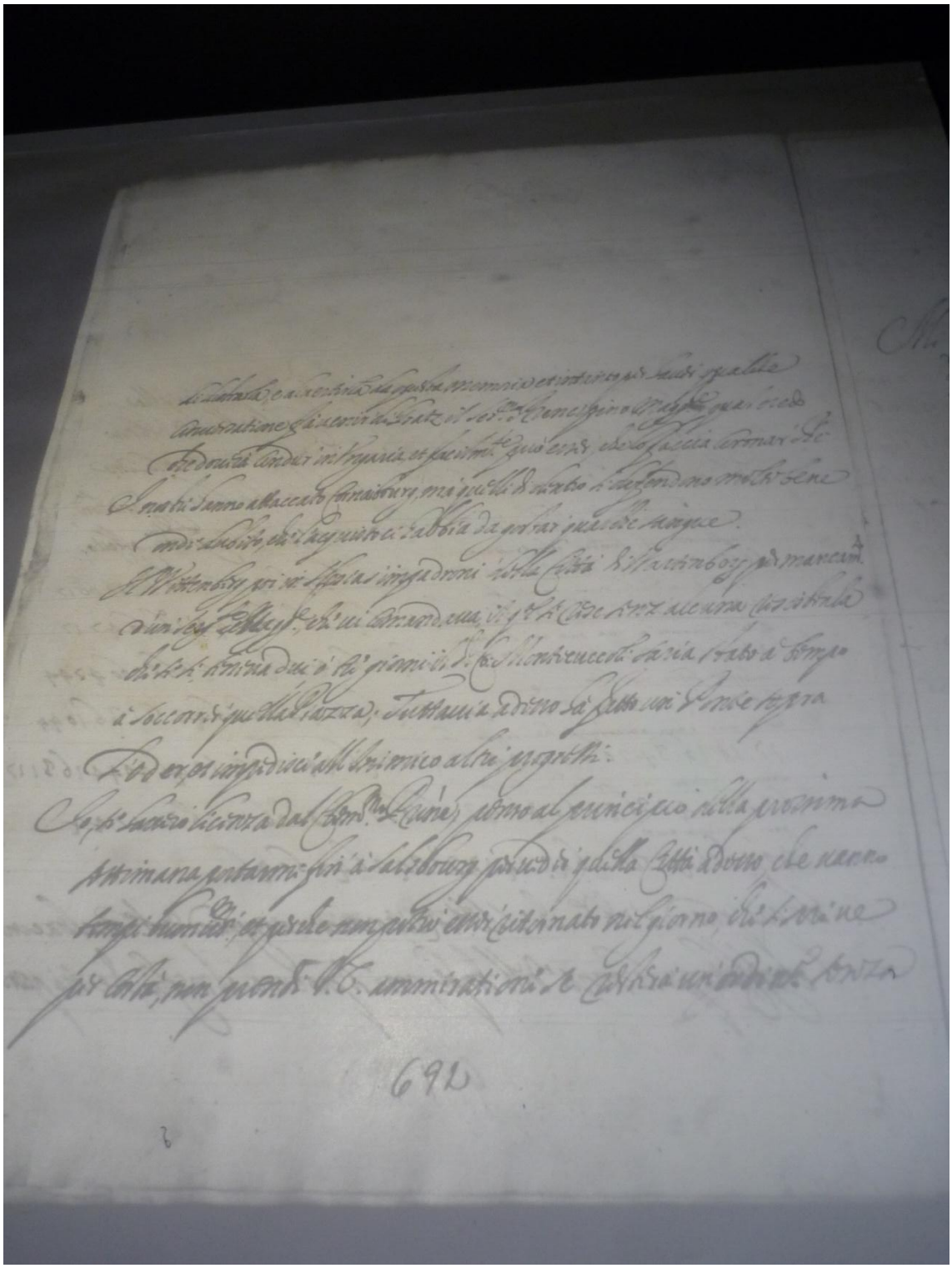


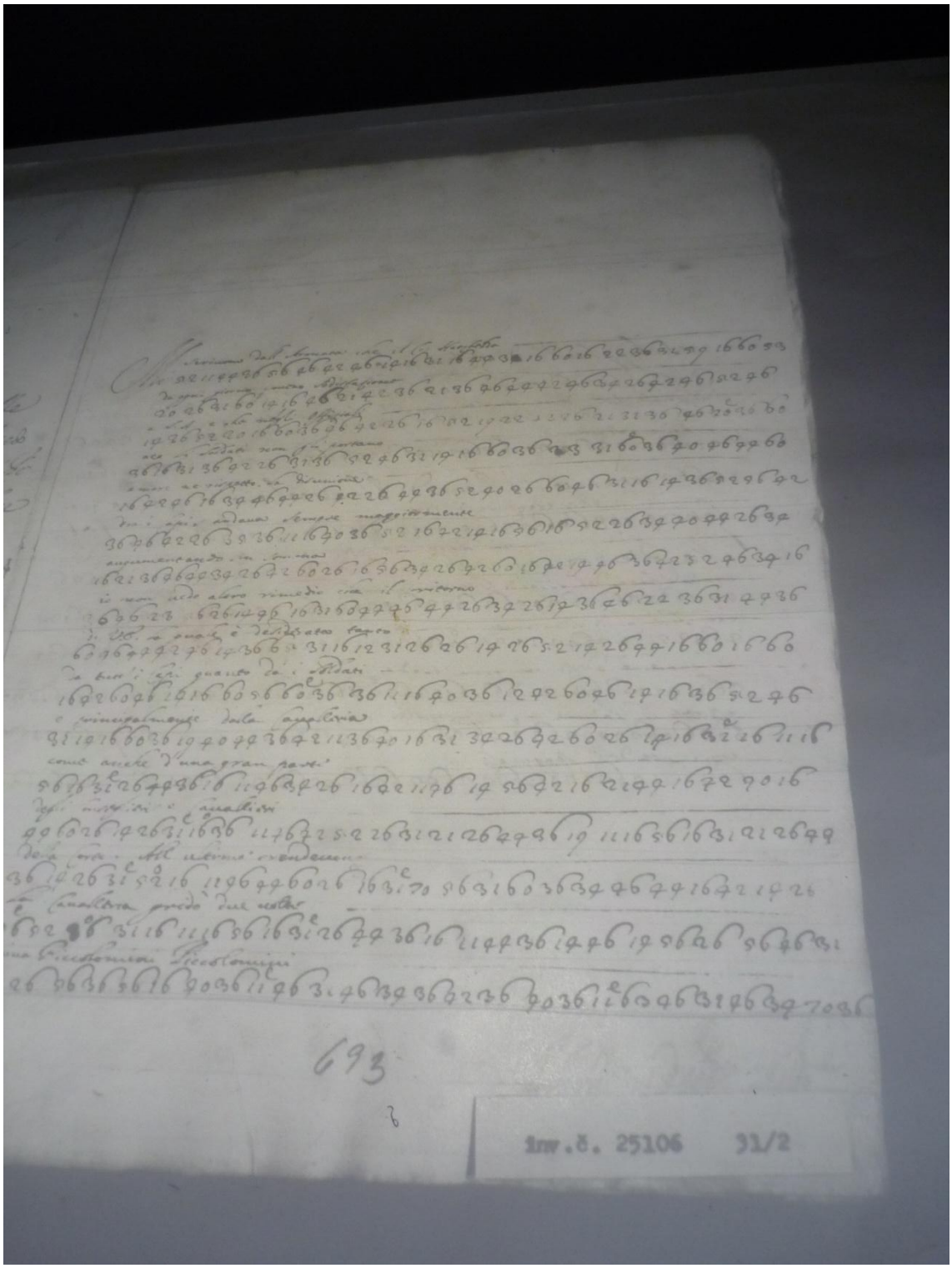


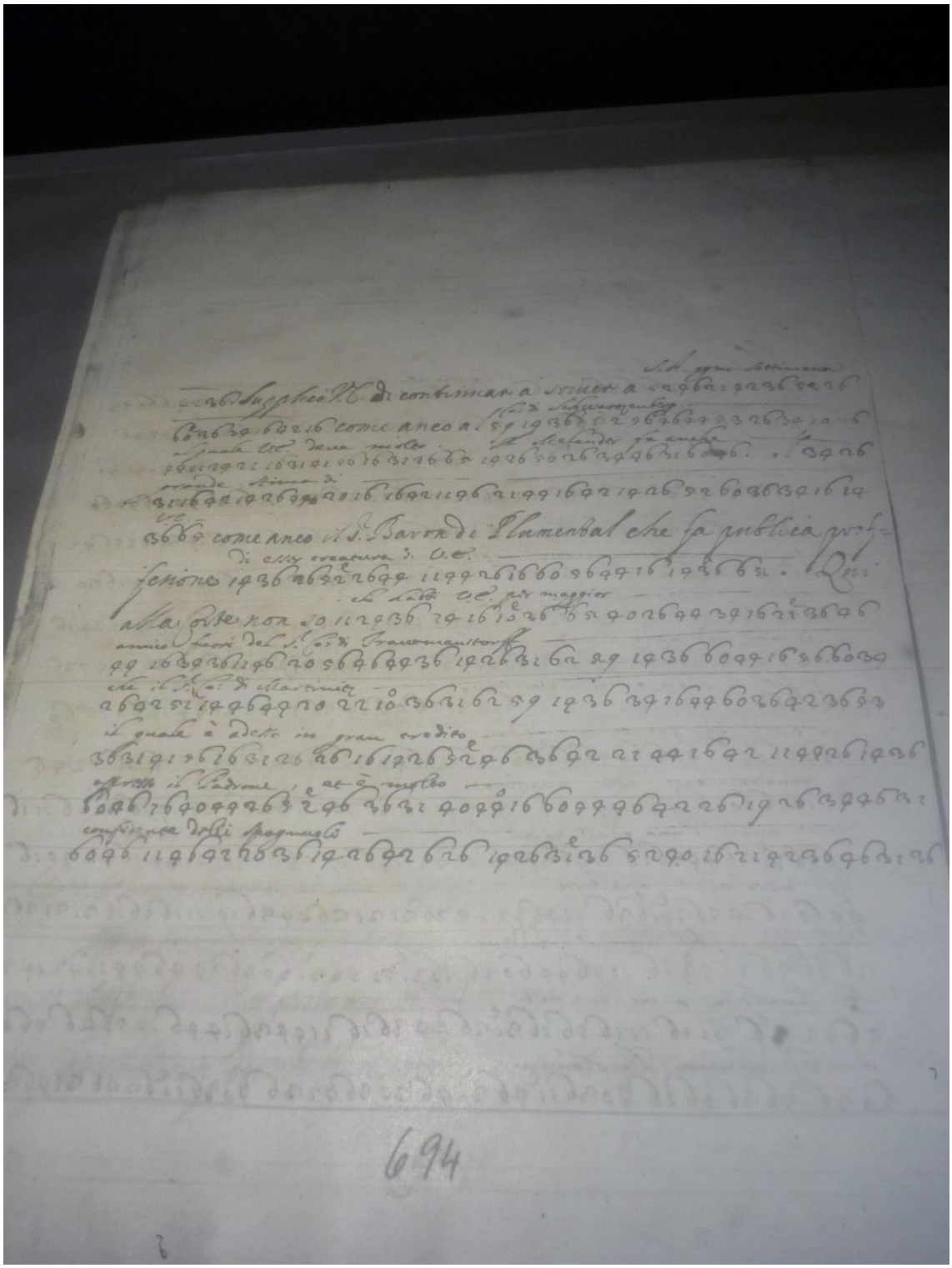









693
inv.s. 25106 31/2



694

B. Fotokopie šifrových textů, které nebyly v práci dešifrovány

(tyto fotokopie jsou přiloženy pouze v elektronické podobě)

B01	Dokument s inventárním číslem 25040
B02	Dokument s inventárním číslem 24784
B03	Dokument s inventárním číslem 24786
B04	Dokument s inventárním číslem 24878
B05	Dokument s inventárním číslem 24788
B06	Dokument s inventárním číslem 24789
B07	Dokument s inventárním číslem 24793
B08	Dokument s inventárním číslem 24794
B09	Dokument s inventárním číslem 24796
B10	Dokument s inventárním číslem 24799
B11	Dokument s inventárním číslem 24799_1
B12	Dokument s inventárním číslem 24800
B13	Dokument s inventárním číslem 24806
B14	Dokument s inventárním číslem 24806_1
B15	Dokument s inventárním číslem 24852
B16	Dokument s inventárním číslem 24852_1
B17	Dokument s inventárním číslem 24853
B18	Dokument s inventárním číslem 24853_1
B19	Dokument s inventárním číslem 24853_2
B20	Dokument s inventárním číslem 24854
B21	Dokument s inventárním číslem 24874
B22	Dokument s inventárním číslem 24876
B23	Dokument s inventárním číslem 24880
B24	Dokument s inventárním číslem 24880_1
B25	Dokument s inventárním číslem 24880_2
B26	Dokument s inventárním číslem 24922
B27	Dokument s inventárním číslem 25026
B28	Dokument s inventárním číslem 25054

B29 Dokument s inventárním číslem 25063
B30 Dokument s inventárním číslem 25065
B31 Dokument s inventárním číslem 25067
B32 Dokument s inventárním číslem 25067_1
B33 Dokument s inventárním číslem 25067_2
B34 Dokument s inventárním číslem 25069
B35 Dokument s inventárním číslem 25069_1
B36 Dokument s inventárním číslem 25071
B37 Dokument s inventárním číslem 25076
B38 Dokument s inventárním číslem 25076_1
B39 Dokument s inventárním číslem 25076_2
B40 Dokument s inventárním číslem 25077
B41 Dokument s inventárním číslem 25079
B42 Dokument s inventárním číslem 25079_1
B43 Dokument s inventárním číslem 25079_2
B44 Dokument s inventárním číslem 25080
B45 Dokument s inventárním číslem 25080_1
B46 Dokument s inventárním číslem 25080_2
B47 Dokument s inventárním číslem 25080_3
B48 Dokument s inventárním číslem 25081
B49 Dokument s inventárním číslem 25081_1
B50 Dokument s inventárním číslem 25081_2
B51 Dokument s inventárním číslem 25081_3
B52 Dokument s inventárním číslem 25081_4
B53 Dokument s inventárním číslem 25081_5
B54 Dokument s inventárním číslem 25082
B55 Dokument s inventárním číslem 25082_1
B56 Dokument s inventárním číslem 25082_2
B57 Dokument s inventárním číslem 25082_3
B58 Dokument s inventárním číslem 25085
B59 Dokument s inventárním číslem 25089
B60 Dokument s inventárním číslem 25089_1
B61 Dokument s inventárním číslem 25090
B62 Dokument s inventárním číslem 25090_1

B63 Dokument s inventárním číslem 25090_2
B64 Dokument s inventárním číslem 25090_3
B65 Dokument s inventárním číslem 25091
B66 Dokument s inventárním číslem 25091_1
B67 Dokument s inventárním číslem 25091_2
B68 Dokument s inventárním číslem 25091_3
B69 Dokument s inventárním číslem 25093
B70 Dokument s inventárním číslem 25093_1
B71 Dokument s inventárním číslem 25093_2
B72 Dokument s inventárním číslem 25099
B73 Dokument s inventárním číslem 25099_1
B74 Dokument s inventárním číslem 25099_2
B75 Dokument s inventárním číslem 25104
B76 Dokument s inventárním číslem 25104_1
B77 Dokument s inventárním číslem 25104_2
B78 Dokument s inventárním číslem 25115
B79 Dokument s inventárním číslem 25115_1
B80 Dokument s inventárním číslem 25115_2