Praktická kryptologie v raném novověku

Jakub Mírka, Státní oblastní archiv v Plzni

CRYPTO 2023, 18. 10. 2023, Policejní akademie ČR, Praha

Velmi stručný nástin vývoje šifrových systémů ve středověké a raně novověké Evropě

- První zmínky o šifrování pochází už ze starověku (Polybiův čtverec, Caesarova a Augustova šifra ad.).
- Již v raném středověku Arabové užívali jednoduché substituce a uměli ji luštit pomocí frekvenční analýzy.
- Ve středověku se kryptologie vyvíjela především v Itálii. První jednoduché nomenklátory s jednoduchou substitucí a několika kódy se objevují již koncem 14. století. V 16. století se např. v papežské korespondenci již běžně užívaly složitější nomenklátory.
- Později se kryptologie dále rozvíjela v románských zemích (kromě Itálie též ve Francii a Španělsku). **Ačkoli již v 16. století existovaly a byly popsány v odborné literatuře velmi důmyslné a složité šifrové systémy, praxi stále vévodila jednoduchá nebo homofonní substituce a nomenklátory.**
- Na sever od Alp pronikaly nové metody později. Ve střední Evropě se v 16. století nejčastěji setkáváme s jednoduchou substitucí, někdy doplněnou o kódy. Podobná situace platí i pro počátek 17. století. Složitější nomenklátory se ve střední Evropě začaly používat spíše až v průběhu třicetileté války.
- V mladší době se čím dál více přecházelo v šifrové abecedě od jiných znaků k číslicím.

Šifrové systémy a jejich historický vývoj

Vybraná literatura:

KAHN, David. *The Codebreakers. The Story of Secret Writing*. New York: Macmillan 1967.

SINGH, Simon. *Kniha kódů a šifer.* Praha: Dokořán a Argo 2003.

JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti.* Praha: Naše vojsko, 1994.

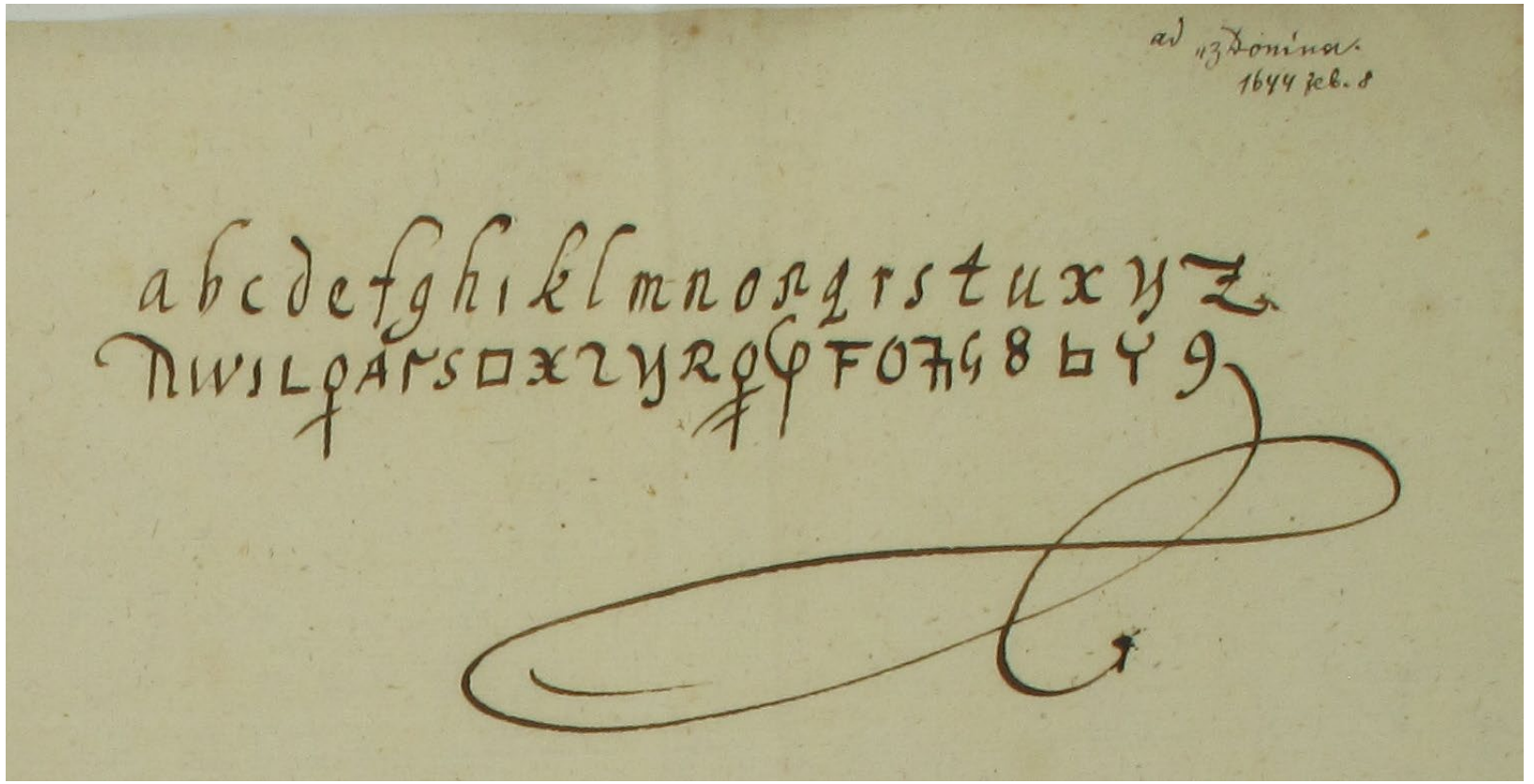
VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros 2006.

KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu.* Praha : Univerzita Karlova 1993, s. 177–209.

Pro stručný přehled dalších prací viz:

MÍRKA, Jakub. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni. *Západočeské archivy 2012*, s. 44–73. Publikováno též v Crypto-World 11, 12/2012, 1,2/2013 a 3, 4/2013 (dostupné z: http://crypto-world.info).

Jednoduchá substituce



Klíč pro šifrování pomocí jednoduché substituce, 1. polovina 17. století,
(Státní oblastní archiv v Plzni, Rodinný archiv Trauttmansdorffů, inv. č. 148)

Nomenklátory a kódové knihy

Nomenklátory byly nejběžnějším šifrovým systémem raného novověku. Často v nich byly kombinovány různé šifrové systémy či prvky.

Nejsložitější nomenklátory obvykle obsahovaly:

a) tabulku jednoduché nebo homofonní substituce,

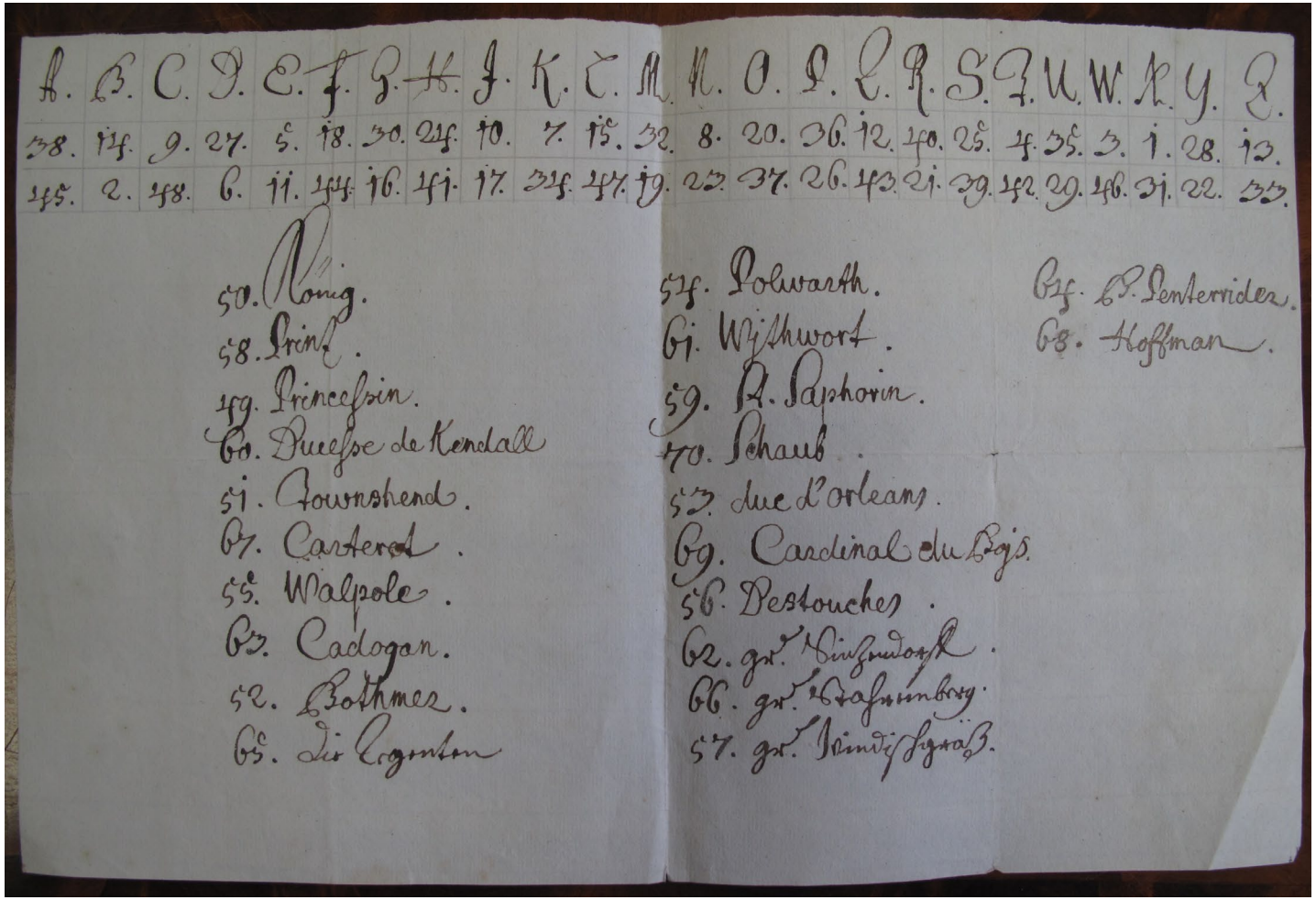
b) část s dvojhláskami nebo jinými bigramy, případně trigramy,

c) klamače (lat. errantes, nullae, literae mutae, angl. nulls),

d) kódy (kódovou knihu).

Kódové knihy byly obvykle sešity (někdy i celé knihy) obsahující desítky až tisíce slov. Často měly podobu nomenklátoru, přičemž ostatní obvyklé náležitosti nomenklátoru (viz výše body a–c) byly zpravidla na první straně.

Jednoduchý nomenklátor

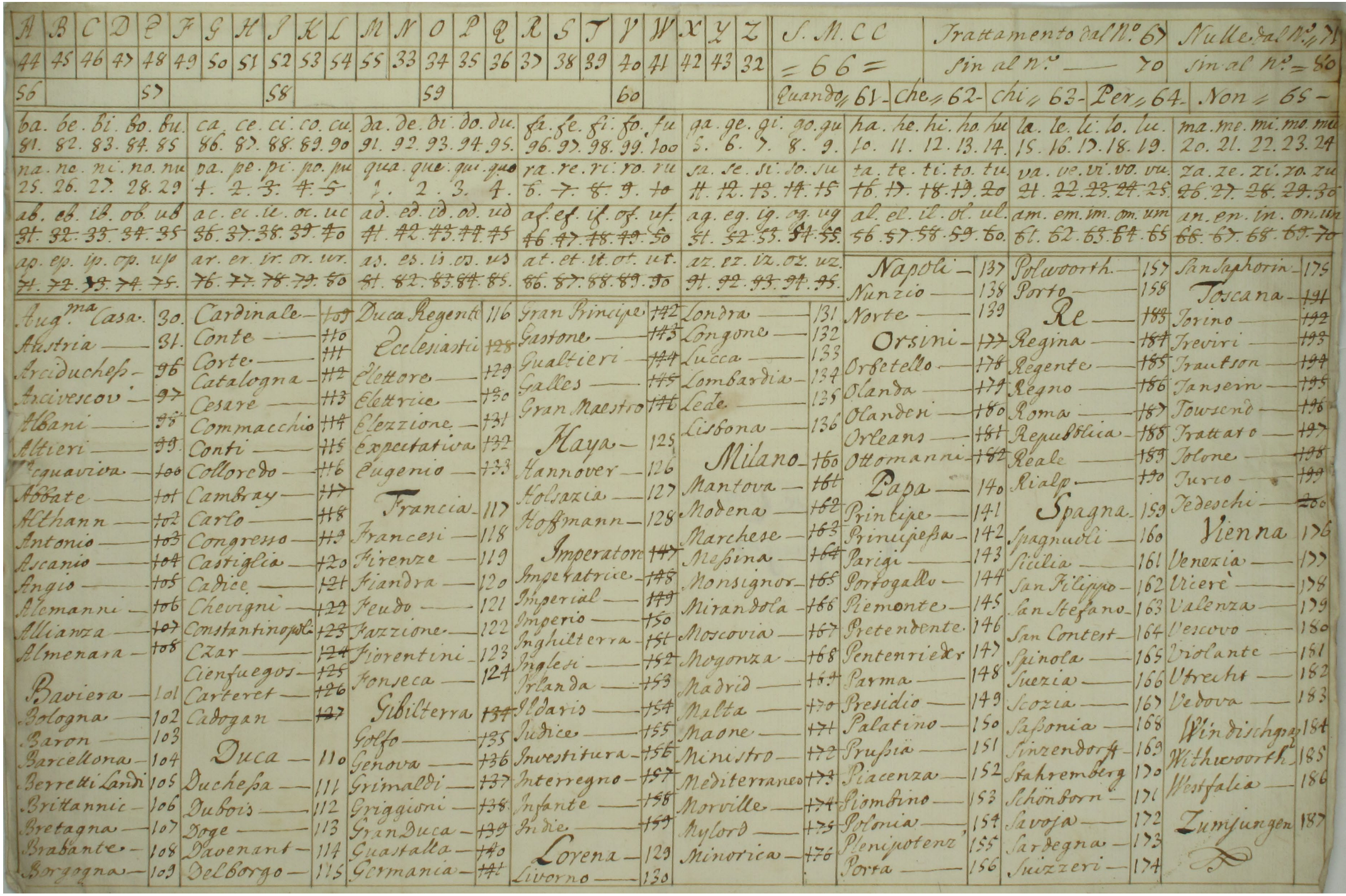


Jednoduchý nomenklátor (homofonní substituce a několik kódů) pro korespondenci s císařským vyslancem v Anglii, pravděpodobně Konrádem Zikmundem hrabětem Starhembergem, cca 1720–1727.
(Státní oblastní archiv v Plzni, Rodinný archiv Windischgrätzů, inv. č. 1403)

Složitý nomenklátor

Nomenklátor pro italsky psanou korespondenci s kardinálem Juanem Álvarem Cienfuegos Villazón, cca 1720–1730.

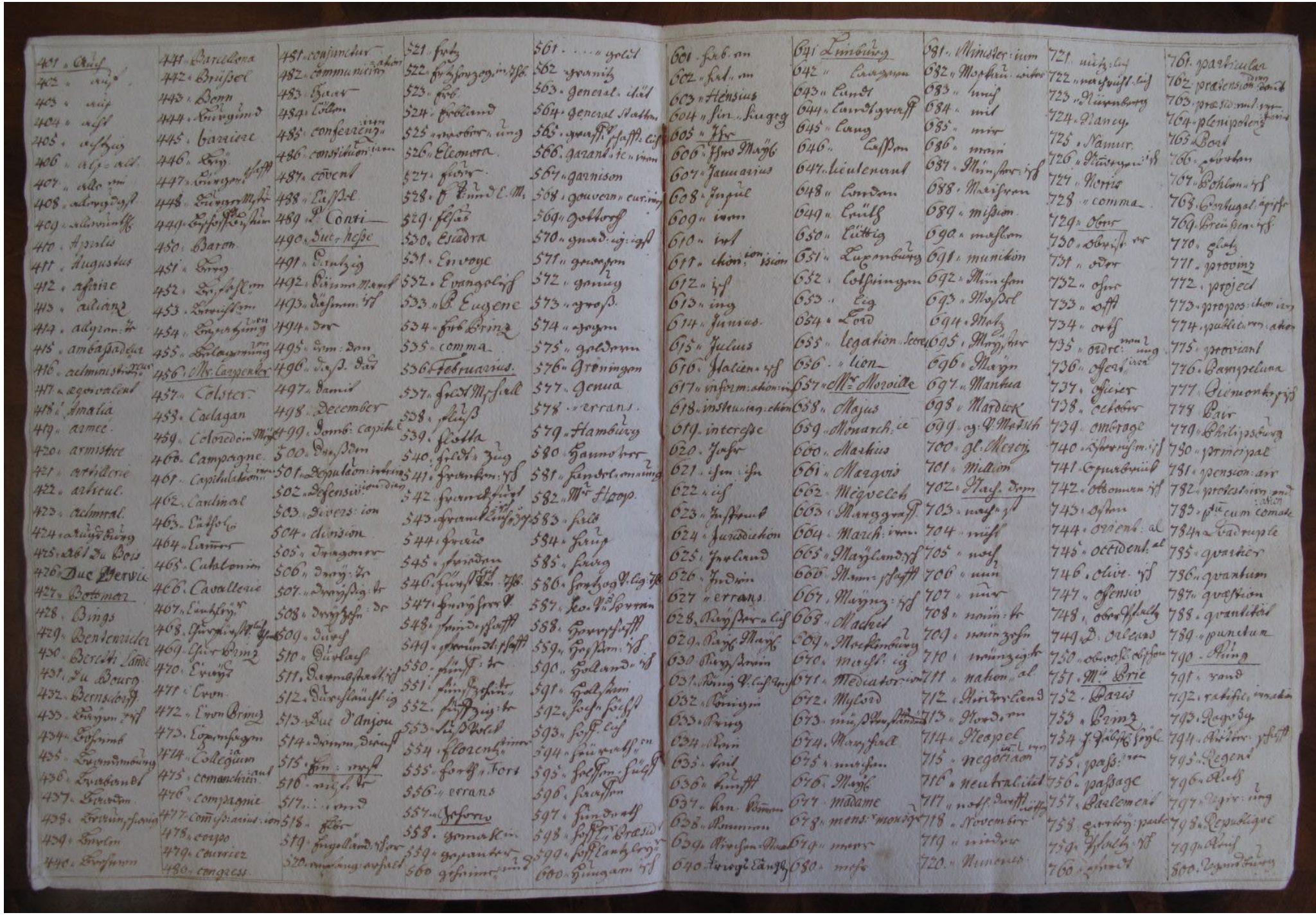
(Státní oblastní archiv v Plzni, Rodinný archiv Windischgrätzů, inv. č. 1403)



Kódová kniha

Nomenklátor kombinovaný s kódovou knihou pro korespondenci s dvorskou tajnou radou ve Vídni.

(Státní oblastní archiv v Plzni, Rodinný archiv Windischgrätzů, inv. č. 1403)



Ukázky šifrované korespondence

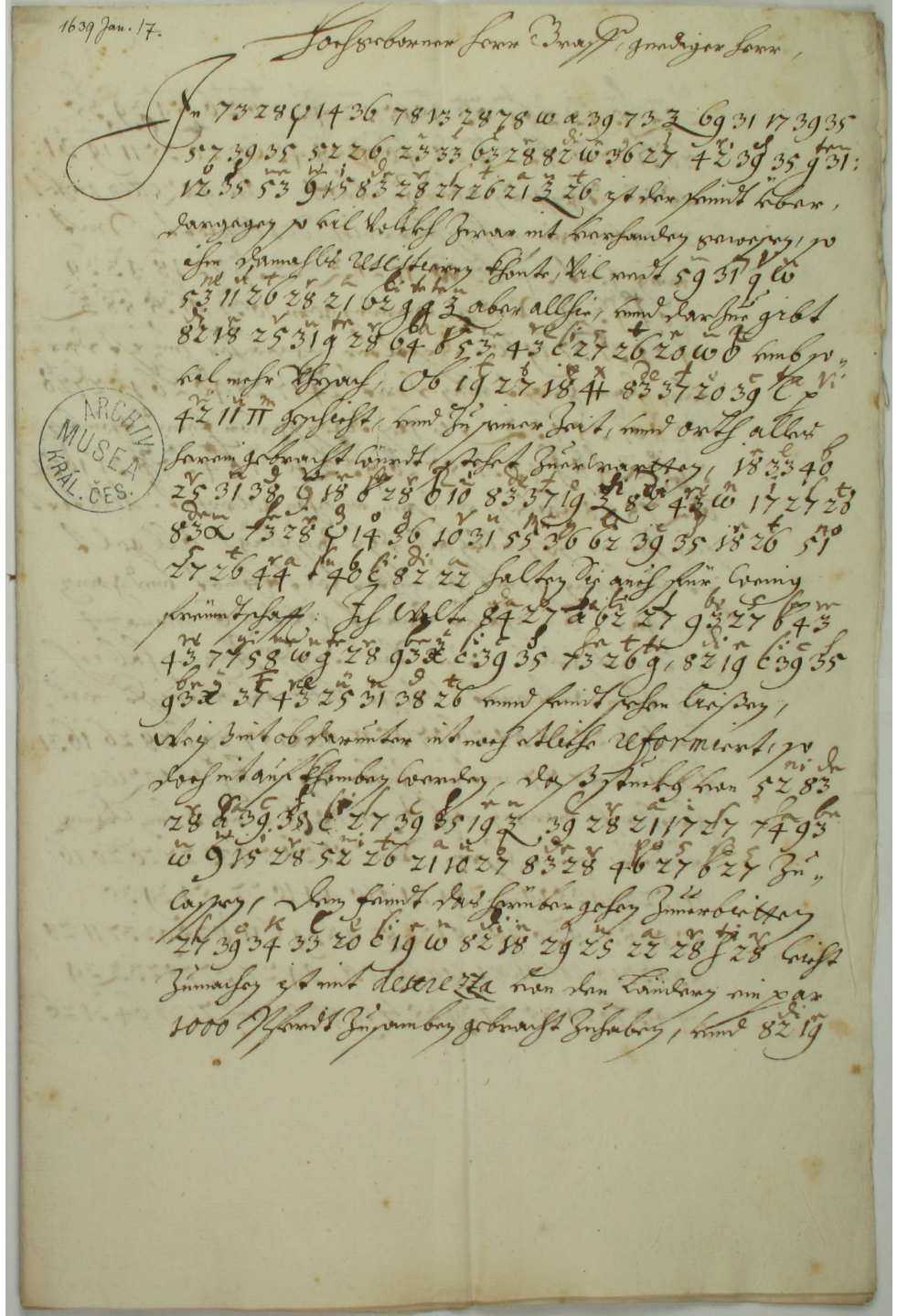
Dopis říšského vicekancléře Ferdinanda Zikmunda Kurtze von Senftenau hraběti Maxmiláno vi z Trauttmansdorffu, 17. ledna 1639

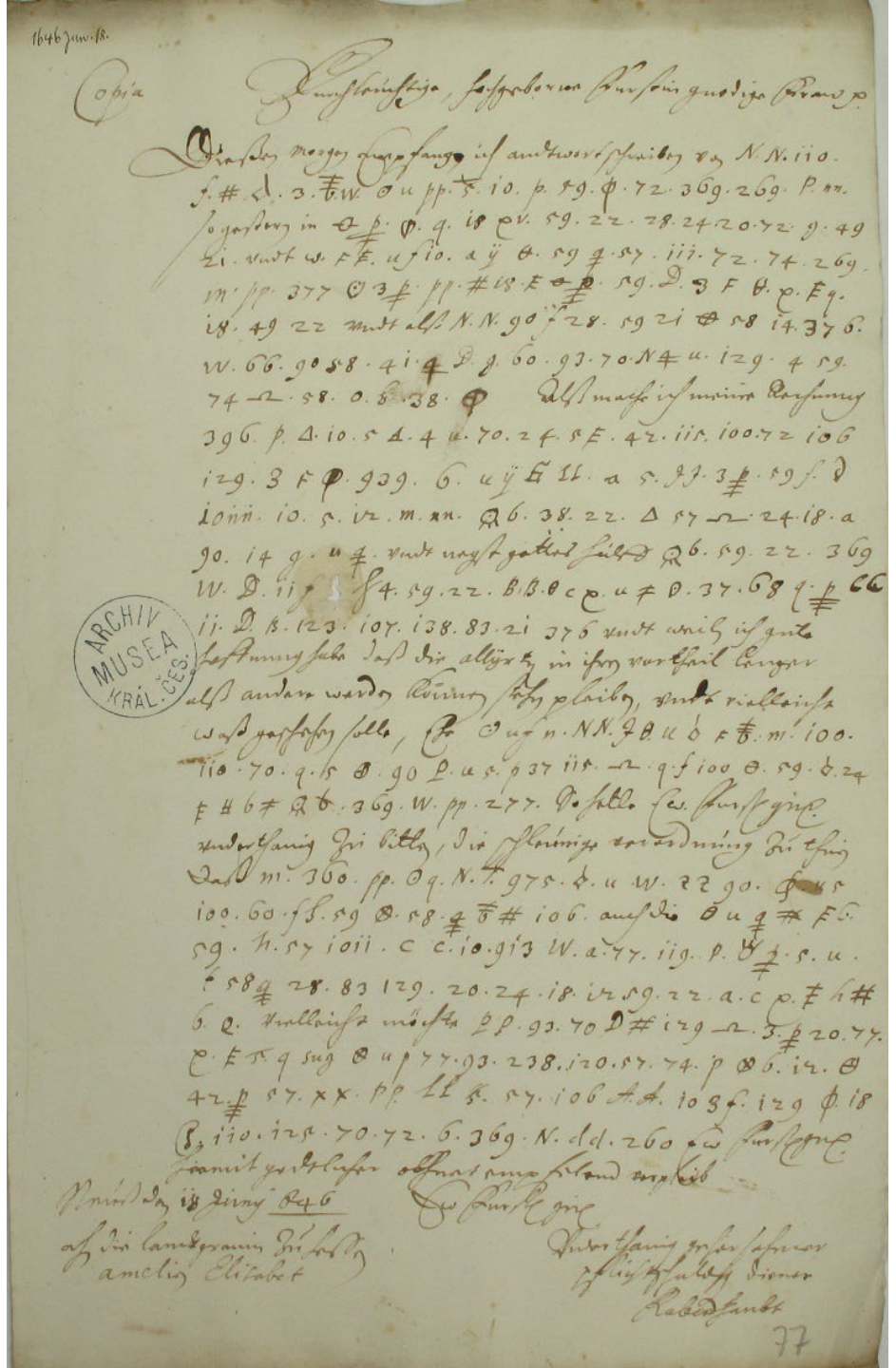
(Státní oblastní archiv v Plzni, Rodinný archiv Trauttmansdorffů, inv. č. 200)

→

Kopie šifrovaného dopisu Karla Rabenhaupta ze Suché, datovaný 11./13. června 1646 (správně má být asi červenec)

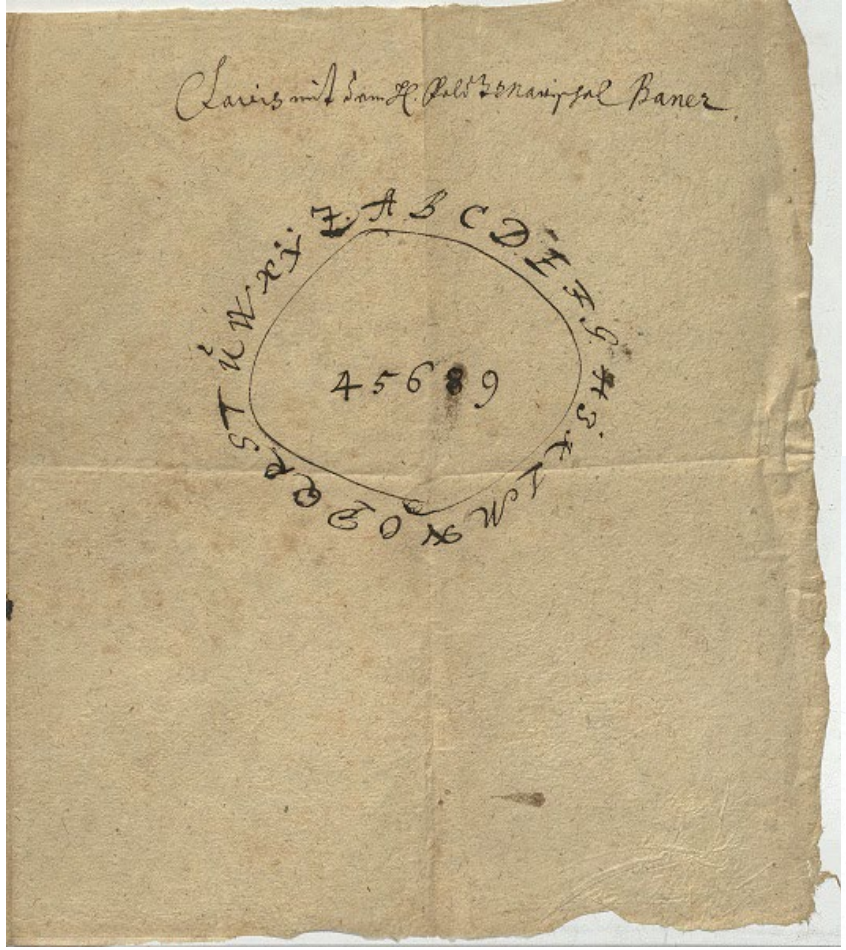
(Státní oblastní archiv v Plzni, Rodinný archiv Trauttmansdorffů, inv. č. 125)





Polyalfabetická substituce

Klíč pro šifrovanou korespondenci se švédským maršálem Johanem Banérem (pravděpodobně polyalfabetická substituce), před 1641 (Hessisches Staatsarchiv Marburg, sign. 4d, Nr. 1918)



→
Šifrovací kotouč pro polyalfabetickou substituci (zdroj: Wikipedia Commons)

Kryptologie ve službě evropských mocností (příklady)

Papežský stát

- koncem středověku a počátkem raného novověku velmi pokročilé způsoby šifrování

MEISTER, Aloys. Die Geheimschrift im Dienste der päpstlichen Kurie. Von ihren Anfängen bis zum des XI. Jahrhunderts. Paderborn 1906. ANTAL,

Benátská republika

- počátkem raného novověku praktické užití kryptologie na vysoké úrovni, v průběhu 17. a 18. století úpadek, stejně jako celé republiky

BUONAVOGLIA, Paolo. Venetian Cryptanalysis Treatises of the Renaissance. In: HistoCrypt 2022 Proceedings of the 5th International Conference on Historical Cryptology, Linköping 2022, s. 22–31.

Černé komnaty:

Francie Ludvíka XIV.

- ve druhé polovině 17. a počátkem 18. století asi nejvýkonnější kryptologická služba

Rakouská „Geheime Ziffernkanzlei“

- ve druhé polovině 18. a první polovině 19. století nejlepší a nejproslulejší služba v Evropě (velmi zdokonaleno šifrování pomocí kódové knihy, zvláště v pozdější době /především za kancléře Metternicha/ společně s policií a státní poštou aparát pro sledování nejen diplomatické pošty, ale též vlastního obyvatelstva, „pobočky“ i v Karlových Varech nebo Mariánských Lázních)

HUBATSCHKE, Harald. Die amtliche Organisation der geheimen Briefüberwachung und des diplomatischen Chiffrendienstes in Österreich. Mitteilungen des Instituts für Österreichische Geschichtsforschung, 1975, s. 352–413.

Šifry v českých archivech

- V zahraničních archivech se obvykle nachází nejvíce šifer v centrálních archivech územních celků, které v období raného novověku tvořily samostatný stát.
- České země nebyly nebyly po většinu této doby (zejména pak po roce 1620), samostatným mocenským a politickým centrem s vlastní vojenskou a zahraniční politikou. Nejvíce šifrovaných dopisů se tedy v českých archivech nachází v rodinných archivech šlechty, zejména v písemných pozůstalostech těch členů rodu, kteří byli významnými diplomaty nebo vojevůdci.
- Příklady šifrovaných pramenů v českých archivech:

(níže uvedené fondy z valné části excerpovány v edici ČECHOVÁ, Gabriela – JANÁČEK, Josef – KOČÍ, Josef – POLIŠENSKÝ, Josef (edd). *Documenta Bohemica Belli Tricennale Illustrantia, Tomus I–VII*. Praha : Academia 1971–1981.)

- Národní archiv: Valdštejniana, Jičín

(ROUBÍK, František. Šifrované dopisy v registratuře Albrechta z Valdštejna. In: *Sborník prací věnovaných prof. Dru Gustavu Friedrichovi k šedesátým narozeninám, 1871–1931*. Praha : Historický spolek v Praze 1931, s. 359–368.)

- SOA Hradec Králové (Zámrsk): Rodinný archiv Piccolominiů, Náchod
- SOA Litoměřice (pobočka Děčín): Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant

(ŠIMSOVÁ, Barbora. Šifrovaná korespondence v písemnostech válečné kanceláře Matyáše Gallase. *Sborník archivních prací*, č. 1, 2, roč. 2019, s. 7–86.)

- SOA Třeboň: Rodinný archiv Buquoyů, sbírky Cizí rody a Historica (v nich šifry Rožmberků)
- SOA Plzeň: Rodinný archiv Trauttmansdorffů, Rodinný archiv Windischgrätzů

(MÍRKA, Jakub. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni. *Západočeské archivy 2012*, s. 44–73.)

- Archiv Národního Muzea: Sbírka D, karton 9

(HANKA, Václav. Correspondenz zwischen Kaiser Rudolf, dem ungarischen Könige Matthias, den Erzherzogen Leopold und Albrecht, dann den Herren Wenceslaw von Wchynicz und Adolf von Althan. Prag 1845.)

Šifry se vztahem k Čechám v zahraničních institucích a mezinárodní databáze šifer

- šifry české provenience, které se dostaly do zahraničí
- korespondence zahraničních panovníků nebo jiných významných osobností se stranami v Čechách (zaznamenány např. v četných četných zprávách o bohemikálních výzkumech v zahraničních archivech, mnohé též opsány nebo digitalizovány)
- písemné pozůstalosti nebo korespondence Čechů, uložená v zahraničí (např. pobělohorští exulanti)

- **Mezinárodní databáze šifrované korespondence a šifrových klíčů:**
  - **DECODE Database** (https://cl.lingfil.uu.se/decode/database/login)

  Obsahuje tisíce klíčů a dopisů. Přesto jde stále jen o zlomek z celku uloženého v evropských paměťových institucích. U většiny nejsou s ohledem na reprodukční práva vidět digitalizáty.
  - **HCPortal** (https://hcportal.eu/)

  Neplní pouze funkci databáze, ale též výukového portálu pro historickou kryptologii. Mnohem méně záznamů než v DECODE, ale u všech jsou digitalizáty. V budoucnu se chystá rozšíření.

Vybrané poznatky získané studiem pramenů

- Pouze malá část z dochované šifrované korespondence je psána českým jazykem, a to dokonce i v případě, že jsou pisateli nebo adresáty Češi.
- Většina šifrované korespondence je buď zcela dešifrovaná, nebo máme k dispozici alespoň část otevřeného textu, díky němuž jsme schopni rekonstruovat klíč a následně dešifrovat zbývající šifrový text.
- Obsahem šifrované korespondence bývají málokdy šokující skutečnosti, které zcela změní náš pohled na konkrétní historické události. Mnohdy jde o zprávy, které sice bylo důležité skrýt v danou dobu před určitými osobami, ale postupem času se potřeba jejich utajení snižovala. Ovšem i dešifrování takových zpráv má význam pro získání uceleného přehledu o obsahu korespondence.
- Samozřejmě ale existují i opačné případy, kdy šifrované pasáže obsahují informace naprosto zásadního významu.

Kryptologická funkce češtiny v zápisnících Alberta Behaima

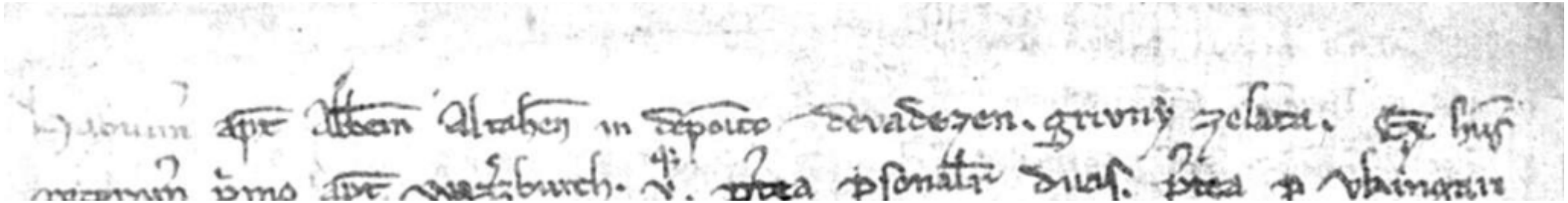
Albert Behaim (Albertus Bohemus), *1190/1195, +1258/1260,

papežský legát a pasovský děkan, stál na papežské straně v opozici proti císaři Fridrichovi II.

Albert Behaim byl snad českého původu, ovšem prokázáno to není. Tuto teorii kromě jeho jména však podporují ojedinělé české pasáže v jeho latinsky psaných zápisnících.

Příklad:

„Habuimus aput abbatem Altahen in deposito devadezen grivny zelata.“



(Münchener DigitalisierungsZentrum, dostupné z: https://www.digitale-sammlungen.de)

Další zdroj informací:

(*Wikipedie: Otevřená encyklopedie: České přípisky v zápisníku Alberta Bohema* [online]. c2020 [citováno 17. 10. 2023]. /zde i další odkazy na literaturu a edici zápisníků/)

Šifrované pasáže v listech Mistra Jana Husa

Na šifrované pasáže v listech mistra Jana Husa upozornil již Václav Novotný.

(*M. Jana Husi Korespondence a dokumenty*. Ed. NOVOTNÝ, Václav. V Praze, 1920.)

Šifrový systém přesněji identifikoval a vysvětlil Bohumil Ryba.

(RYBA, Bohumil. K tajnému písmu v listech Husových. *Sborník historický* 1, 1953, s. 46–52.)

Práce na odhalení šifrového systému byly ztíženy tím, že se nedochovaly originální Husovy dopisy, ale jen jejich opisy.

Dopisy jsou psány jak v latině, tak v češtině.

Husem užívaný šifrový systém

Hus nahrazoval pouze samohlásky, a to písmenem bezprostředně následujícím:

a → b | e → f | i → k | o → p | u → x | y → z

Husem užívaná abeceda:

a b c d e f g h i k l m n o p q r s t v/u x y z

Znak „v“ se užíval i pro „u“, dvojité „w“ pak psal jako „vv“ a šifroval „xx“.

Příklad užití:

OT: Vyclef	OT: uherský	OT: VVēc^{e} (tj. Wenceslae)
ŠT: xzclff	ŠT: xhfrskz	ŠT: xxfcf

Tento systém nebyl unikátním systémem Husovým. Patrně byl relativně známý mezi středověkými učenci a Bohumil Ryba poskytl několik příkladů jeho užití i v jiných pramenech.

Šifrovaná korespondence Petra Voka z Rožmberka

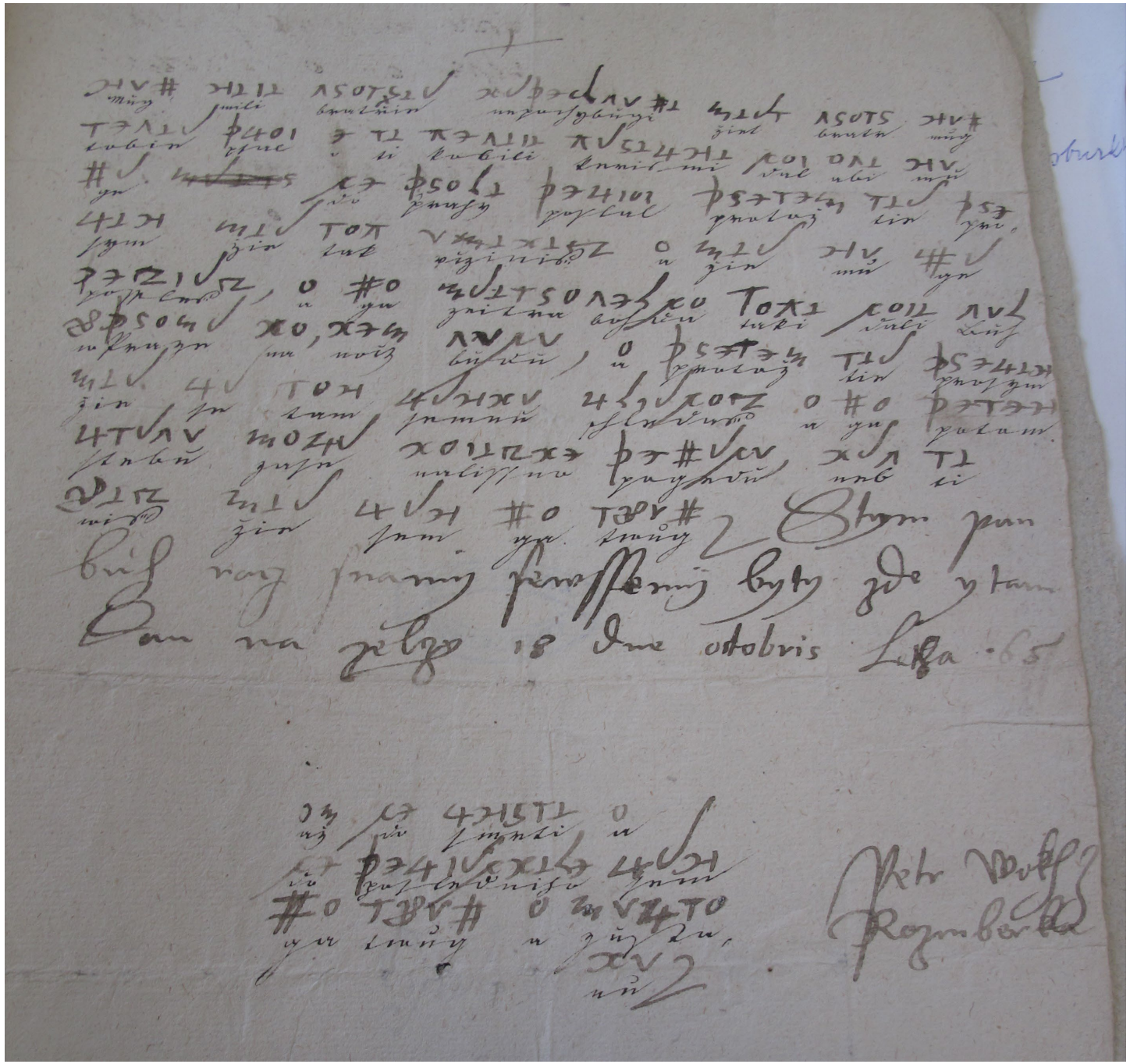
- Petr Vok z Rožmberka (1539–1611) byl v letech 1592–1611 poslední vladař rožmberského domu.
- Korespondence Petra Voka uložena ve Státním oblastním archivu v Třeboni ve sbírce Cizí rody.
- Pomineme-li Husův jednoduchý systém, jsou šifrované dopisy Petra Voka z Rožmberka nejstarší mně známý doklad užití uceleného šifrového systému pro utajení textu psaného v českém jazyce. Nejstarší mně dosud známý dopis je z roku 1565.

- Známa je i korespondence Petra Voka z doby kolem roku 1610 s Janem Jiřím I. Anhaltsko-Desavským. Ta byla v minulosti opsána českými archiváři v Anhaltském státním archivu v Zerbstu a vybrané opisy jsou nyní součástí Sbírky opisů a kopií archiválií v Národním archivu (šifrovaná korespondence se nachází zejména pod sign. Zerbst A 9a, čís. 159).

(HULEC, Otakar. Konspirativní charakter předbělohorské protistavovské opozice. *Jihočeský sborník historický* 30, 1961, s. 97–102.)

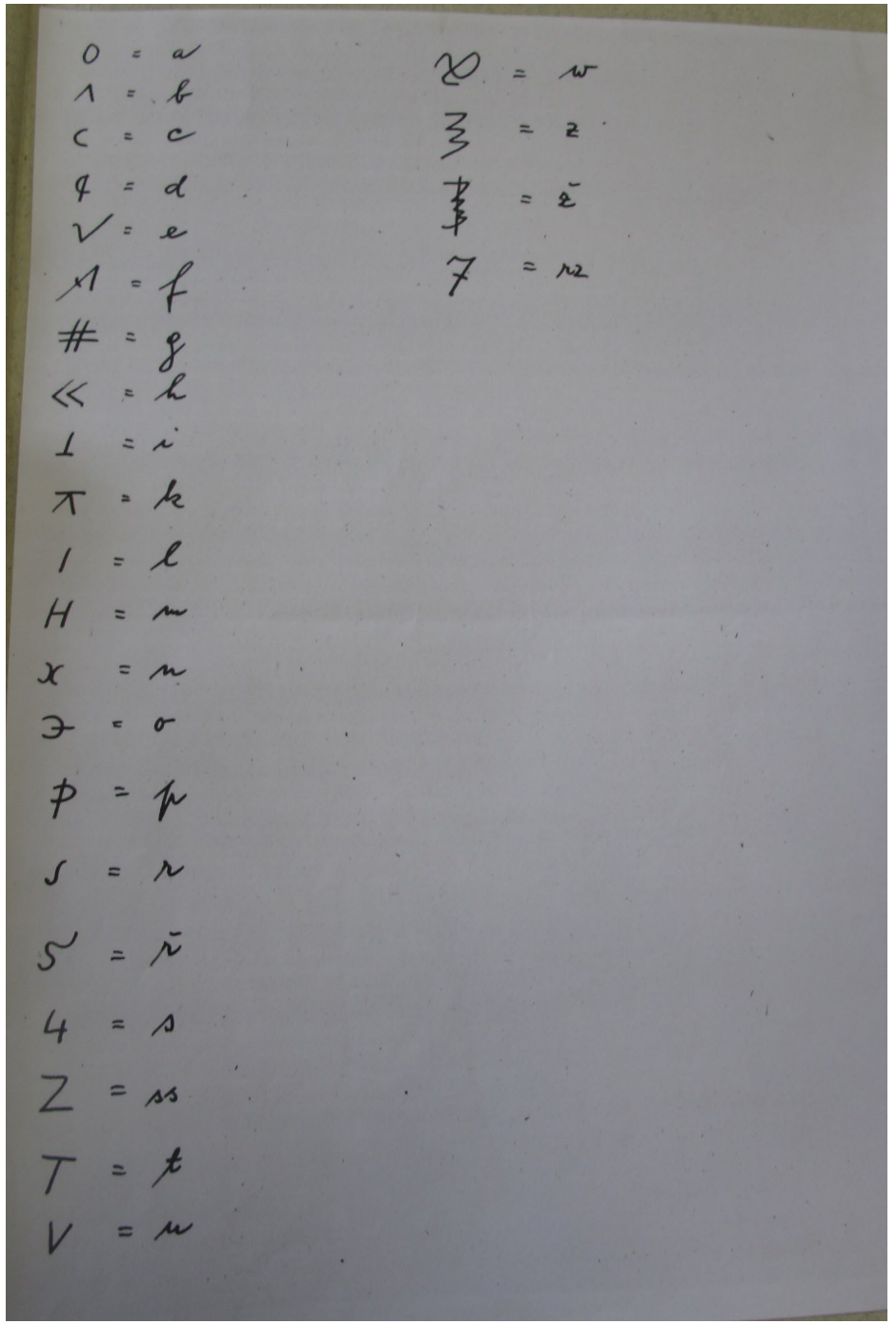
Petr Vok z Rožmberka píše Václavovi Holickému ze Šternberka, 1565

(Státní oblastní archiv v Třeboni, Cizí rody, z Rožmberka 21)



Klíč k šifrované korespondenci
(rekonstruovaný v mladší době)

(Státní oblastní archiv v Třeboni,
Cizí rody, z Rožmberka 17)



Transliterace dešifrovaného textu dopisu Václavu Holickému ze Šternberka z roku 1565

(pro lepší přehlednost doplněna interpunkce)

Mug mili bratrzie nepoch[y]buji, ziet bratr mug
tobie psal o ti kobili keris mi dal, abi mu
ge do Prahy poslal, protoz tie pro-
sim, zie tak uciniss a zie mu ge
possless, a ga zeitra bohda taki, dali Buh,
w Praze na no[c]z budu, a protoz tie prosim,
zie se tam semnu shledass a ja potom
stebu zase na Lissno pogedu, neb ti
viss zie sem ga twug. S tym pan
Buh racz snamy sewssemy byty zde y tam.
Dan na Zelczy 18. dne octobris Letha 65.

Az do smrti a
do posledniho sem
ga twug a zusta-
nu

Petr Wokh z
Rozmberka

Šifrovaná korespondence Viléma z Rožmberka

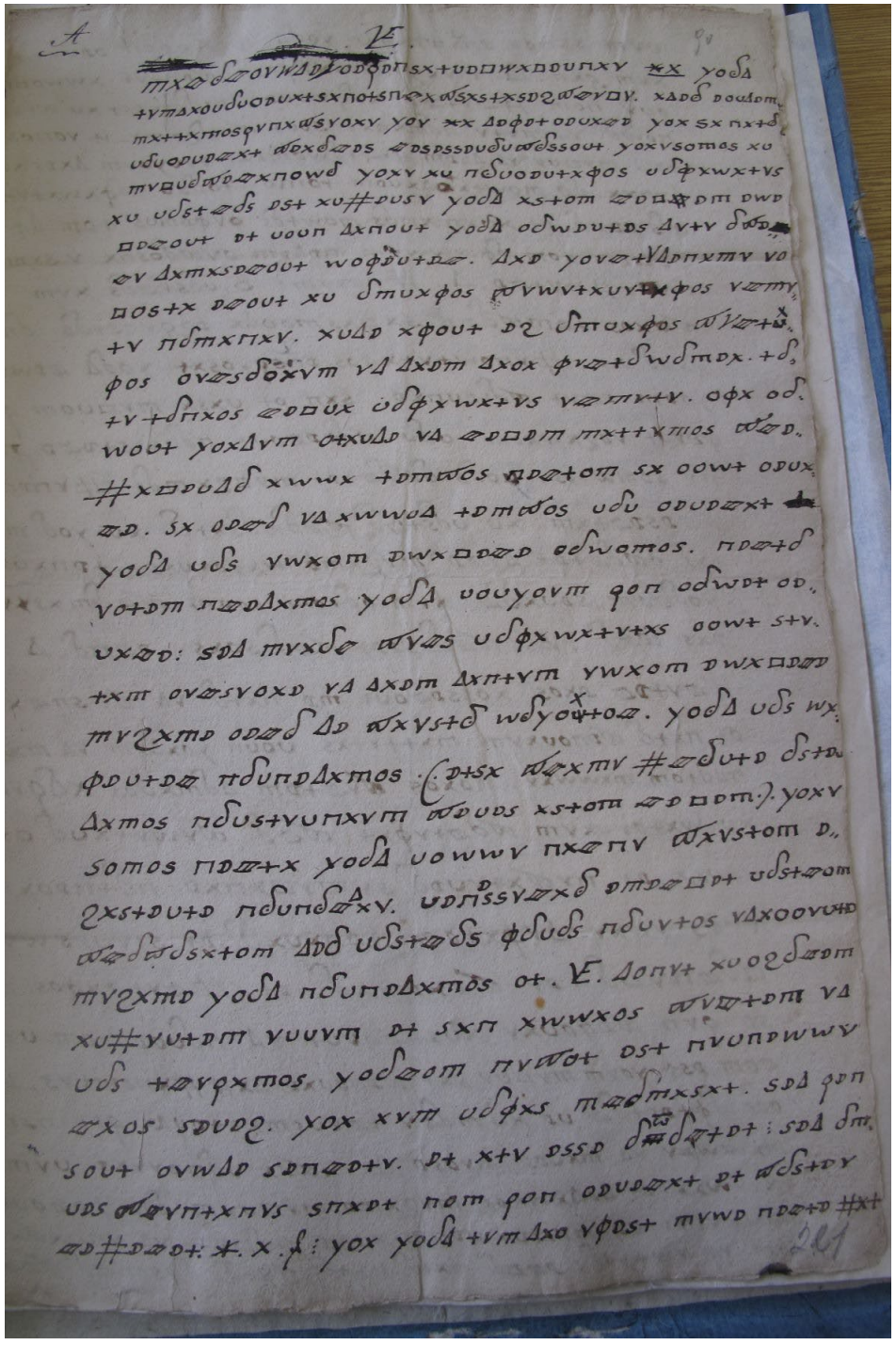
- Vilém z Rožmberka (1535–1592), starší bratr Petra Voka, v letech 1551–1592 vladař rožmberského domu

- V 70. letech 16. století byl po vymření Jagellonců po meči jedním z kandidátů na polský trůn. Při této příležitosti komunikoval také pomocí šifrovaných zpráv. Ta to korespondence je také uložena ve Státním oblastním archivu v Třeboni ve sbírce Historica.

- Korespondence vedena především v latině.

Ukázka šifrované latinské zprávy z doby kandidatury Viléma z Rožmberka na polský trůn

(Státní oblastní archiv v Třeboni, Historica, sign. 4834/36)



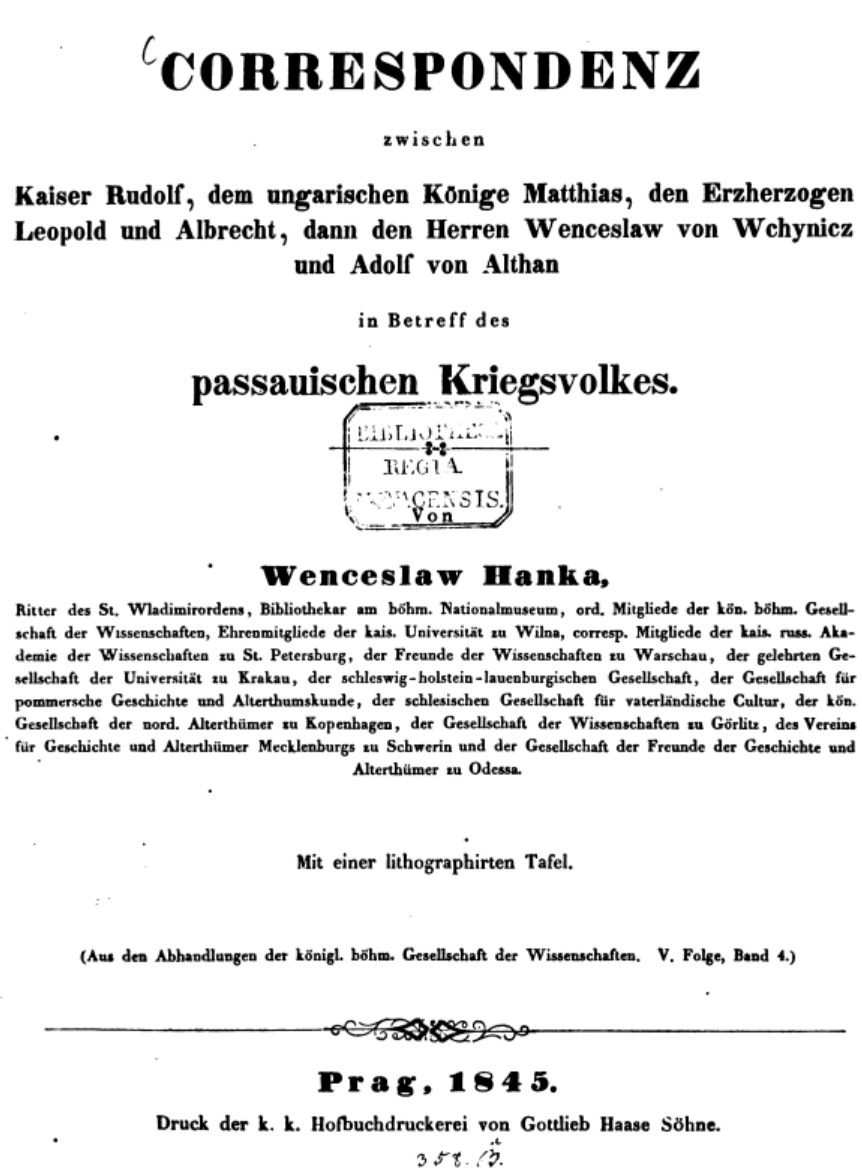
Rekonstrukce klíče k šifrované korespondenci Viléma z Rožmberka

(převzato z VERŽOVSKIJ, Fedor. *Dve kandidatury na polskij prestol Vilgelma iz Rozenberga i ercgercoga Ferdinanda 1574–1575 po neizdannym istočnikam*. Varšava : Tipografija K. Kovalevskago 1889, s. 73)

Šifrovaná korespondence císaře Rudolfa, maďarského krále Matyáše, arcivévodů Leopolda a Albrechta a pánů Václava z Vchynic a Adolfa von Althan ve věci vpádu Pasovských

- Dopisy pocházejí z let 1608–1611.
- Jen část z nich je šifrovaná.
- Dopisy byly původně ve vlastnictví Václava Hanky, který je z větší části dešifroval a publikoval jejich edici.
- Nyní jsou sočástí Sbírky D (karton 9) Archivu Národního muzea.
- Je zde větší množství česky psaných dopisů, některé z nich jsou však pouze dobové překlady do češtiny, vyhotovené Albertem z Kaménka.
- Jeden Hankou nerozluštěný dopis vyluštil Antonín V. Maloch.

(MALOCH, Antonín V. Rozluštění chiffrovaného písma v češtině. *Lumír* 1858, s. 205–206)



CORRESPONDENZ

zwischen

Kaiser Rudolf, dem ungarischen Könige Matthias, den Erzherzogen Leopold und Albrecht, dann den Herren Wenceslaw von Wchynicz und Adolf von Althan

in Betreff des

passauischen Kriegsvolkes.

Wenceslaw Hanka,

Ritter des St. Wladimirordens, Bibliothekar am böhm. Nationalmuseum, ord. Mitgliede der kön. böhm. Gesellschaft der Wissenschaften, Ehrenmitgliede der kais. Universität zu Wilna, corresp. Mitgliede der kais. russ. Akademie der Wissenschaften zu St. Petersburg, der Freunde der Wissenschaften zu Warschau, der gelehrten Gesellschaft der Universität zu Krakau, der schleswig-holstein-lauenburgischen Gesellschaft, der Gesellschaft für pommersche Geschichte und Alterthumskunde, der schlesischen Gesellschaft für vaterländische Cultur, der kön. Gesellschaft der nord. Alterthümer zu Kopenhagen, der Gesellschaft der Wissenschaften zu Görlitz, des Vereins für Geschichte und Alterthümer Mecklenburgs zu Schwerin und der Gesellschaft der Freunde der Geschichte und Alterthümer zu Odessa.

Mit einer lithographirten Tafel.

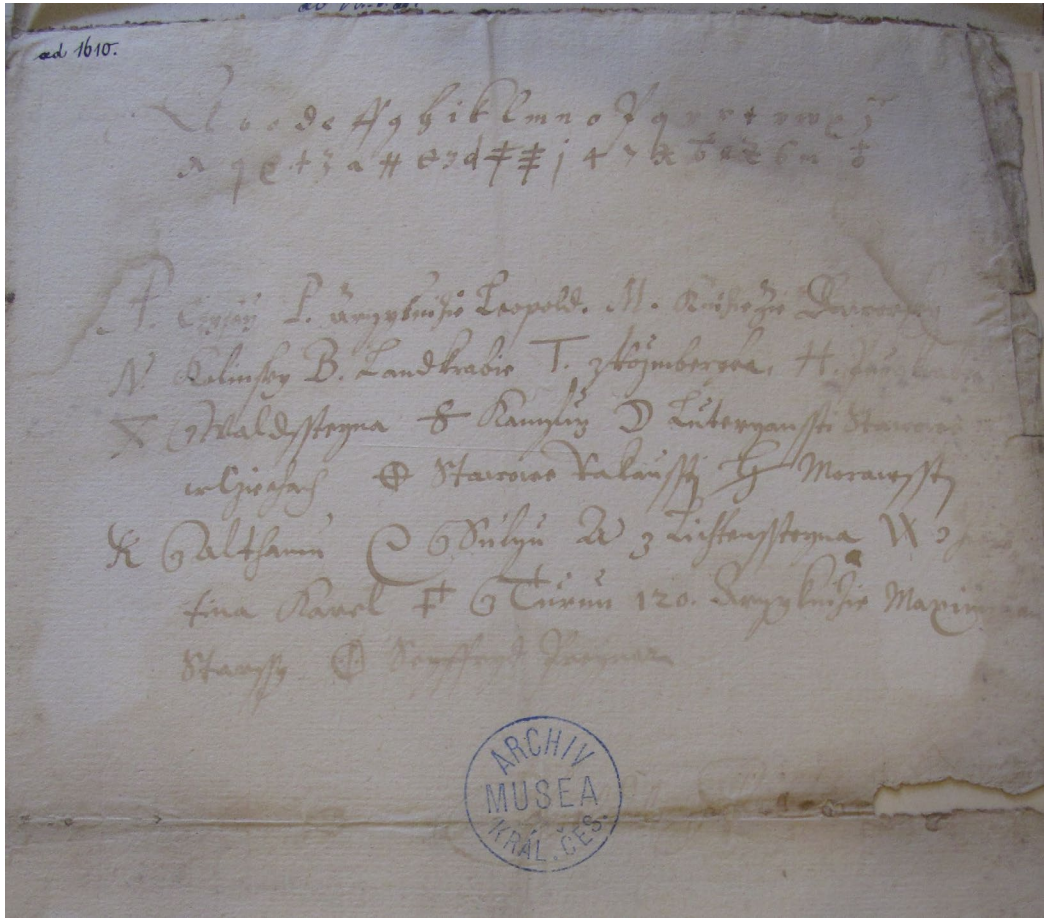
(Aus den Abhandlungen der königl. böhm. Gesellschaft der Wissenschaften. V. Folge, Band 4.)

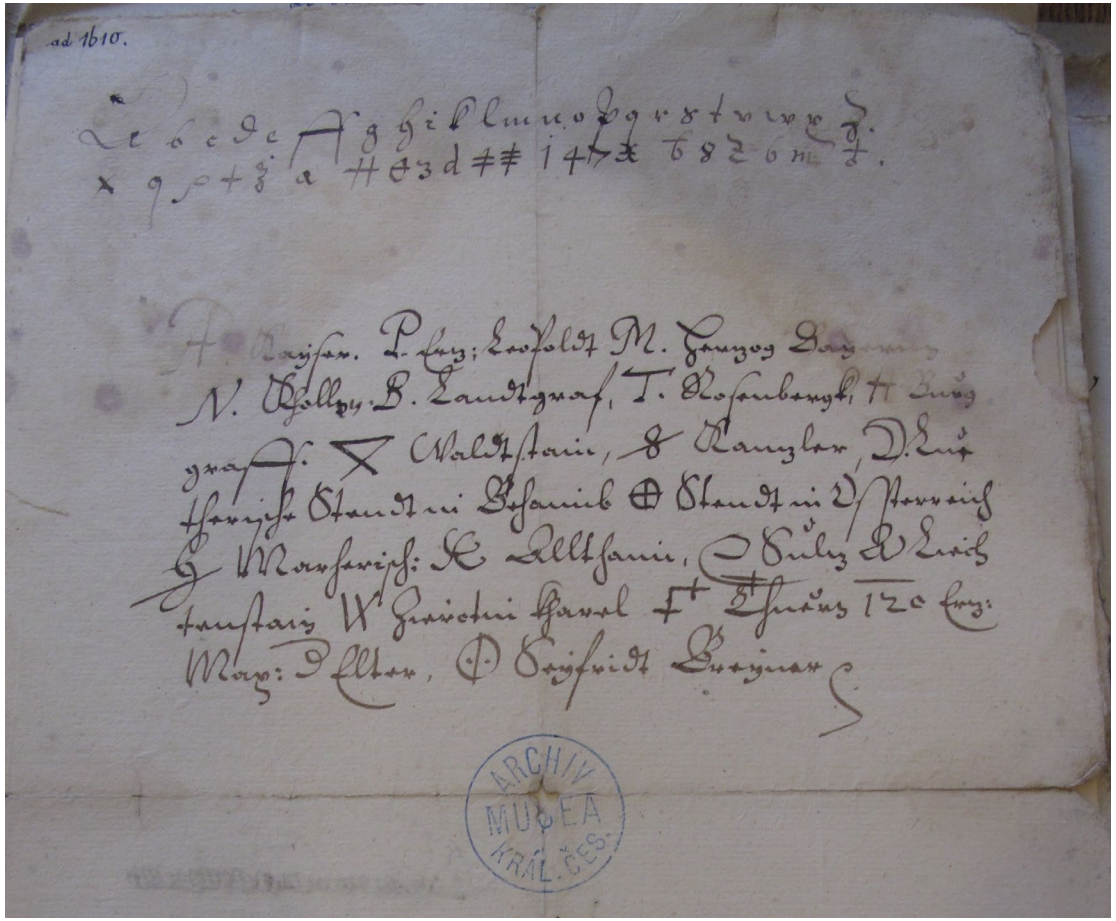
Prag, 1845.

Druck der k. k. Hofbuchdruckerei von Gottlieb Haase Söhne.

(HANKA, Václav. *Correspondenz zwischen Kaiser Rudolf, dem ungarischen Könige Matthias, den Erzherzogen Leopold und Albrecht, dann den Herren Wenceslaw von Wchynicz und Adolf von Althan.* Prag 1845 /titulní list/)

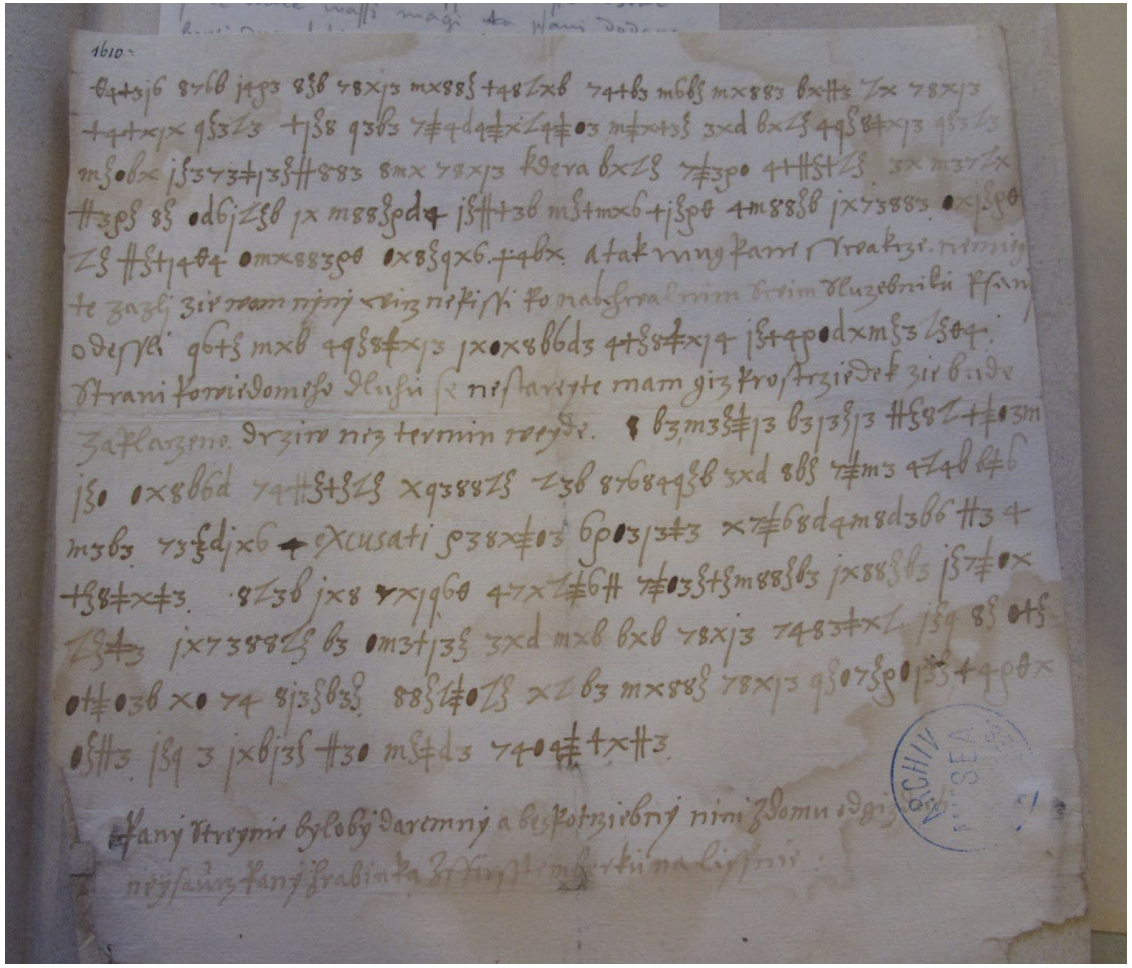
Jeden z klíčů ze Sbírky D v ANM (česká a německá verze téhož klíče)





(Archiv Národního muzea, Sbírka D, karton č. 9.)

Anonymní šifrovaný dopis (lze dešifrovat podle předchozího klíče)



(Archiv Národního muzea, Sbírka D, karton č. 9.)

s. 40

Cifry.

Hodinu s půl noci sem psaní waše dostal; podle wůle waší mají ta psaní doddna býti, dnes byli prokoratoři w radě jak máte obesláni býti, wezma nejpilnější swá psaní, která máte

s. 41

pryč odjeti, já wyptajíc se z Kuntem na wšecko nejdýl we dwau dnech owšem napiši, zanechte jednoho z wašich za sebau doma. A tak můj Pane swakře, nemějte za zlé, že wám nyní wic, nepíši, po naschwálním swém služebníku psaní odešli: *bude Wám obeslání na Zásmuky odesláno, nedočkdwejte ho.* Strany powědomého dluhu se nestarejte, mám již prostředek, že bude zaplaceno, dřiwe než termín wejde. *Mé wěrné mínění jest, dřiw než do Zásmuk pojedete, abyste tím způsobem, jak sme prwé o tom mluwili, pěknau excusati císaři učinili, a Pruskowskému ji odeslali; s tím nds Pán bůh opatruj předewšemi našimi nepřátely, napište mi z Widně, jak tam mám psaní poslati, neb se zde zdržím až po sněmě, šetřte aby waše psaní bezpečně dochazeli, neb i na mne již weliký pozor dají.*

Paní Strejni byloby daremné a bezpotřebné nyní z domu odjížděti, nejsauc ani hrabinka z furštenberku na lišně.

(HANKA, Václav. *Correspondenz* …, s. 40–41.)

Constructio sive Strues Trithemiana
(první známá česká kryptografická příručka)

Autorem příručky je **Rafael Soběhrd Mnišovský ze Sebuzína a Herštejna**
(*1580 v Horšovském Týně, +1644 v Praze)

- právník, studoval v Paříži a Římě
- vychovatel pozdějšího císaře Ferdinanda III., kterého naučil česky
- někdy označován za potenciálního autora Voynichova rukopisu
- autor kryptografické příručky Constructio sive Strues Trithemiana
- ta byla odvezena Švédy v závěru třicetileté války a je uložena v Uppsale
- již roku 1796 na rukopis upozornil Josef Dobrovský, který ji považoval za gramatickou příručku
- na skutečnost, že jde o kryptologickou příručku upozornila první Carin Davidssonová

Vybraná literatura k tématu:

KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu.* Praha : Univerzita Karlova 1993, s. 189–190.

DAVIDSSON, Carin. Johannes Trithemius' Polygraphia als tschechisches Lehrbuch. Cod. Slav. 60 bei der Universitätsbibliothek in Uppsala. *Scando–Slavica 5*, 1959, s. 148–164.

VONDRUŠKA, Pavel. První česká kryptografická příručka. *Crypto-World* 1/2008, s. 18–20. (dostupné z: http://crypto-world.info)

Ukázka z díla Constructio sive Strues Trithemiana

(převzato z VONDRUŠKA, Pavel. První česká kryptografická příručka. *Crypto-World* 1/2008, s. 18–20.)

nás všech. L.

hříchy	a	scelera
provinění	b	dulicta
dopuštění	c	culpae
vejstupení	d	transgressiones
zlosti	e	iniquitates
nepravosti	f	facinora
nečistoty	g	immunditiae
zahálení	h	negligentiae
zanedbání	i	omissiones
nedbanlivosti	k	incuriae
opouštění	l	ignaviae
nespravedlnosti	m	iniustitiae
činy	n	facta
skutky	o	opera
zlá myšlení	p	cogitationes
praktiky	q	practicae
omyly	r	errores
šibalství	s	nequitiae
fortele	t	dolus
zlé zachování	u	noxae
zlé chování	w	excessus
poskvrny	x	nauae(?)
zlé živobytí	y	victum malum
přestoupení	z	reatus

omnium nostrum. L.

Ukázka a přepis jedné ze stránek rukopisu (fol. 61v) .

Šifrovaná korespondence Albrechta z Valdštejna

- Korespondence Albrechta z Valdštejna je uložena v Národním archivu

(Národní archiv, Valdštejniana, Jičín, inv. č. 16847–16915, karton 89)

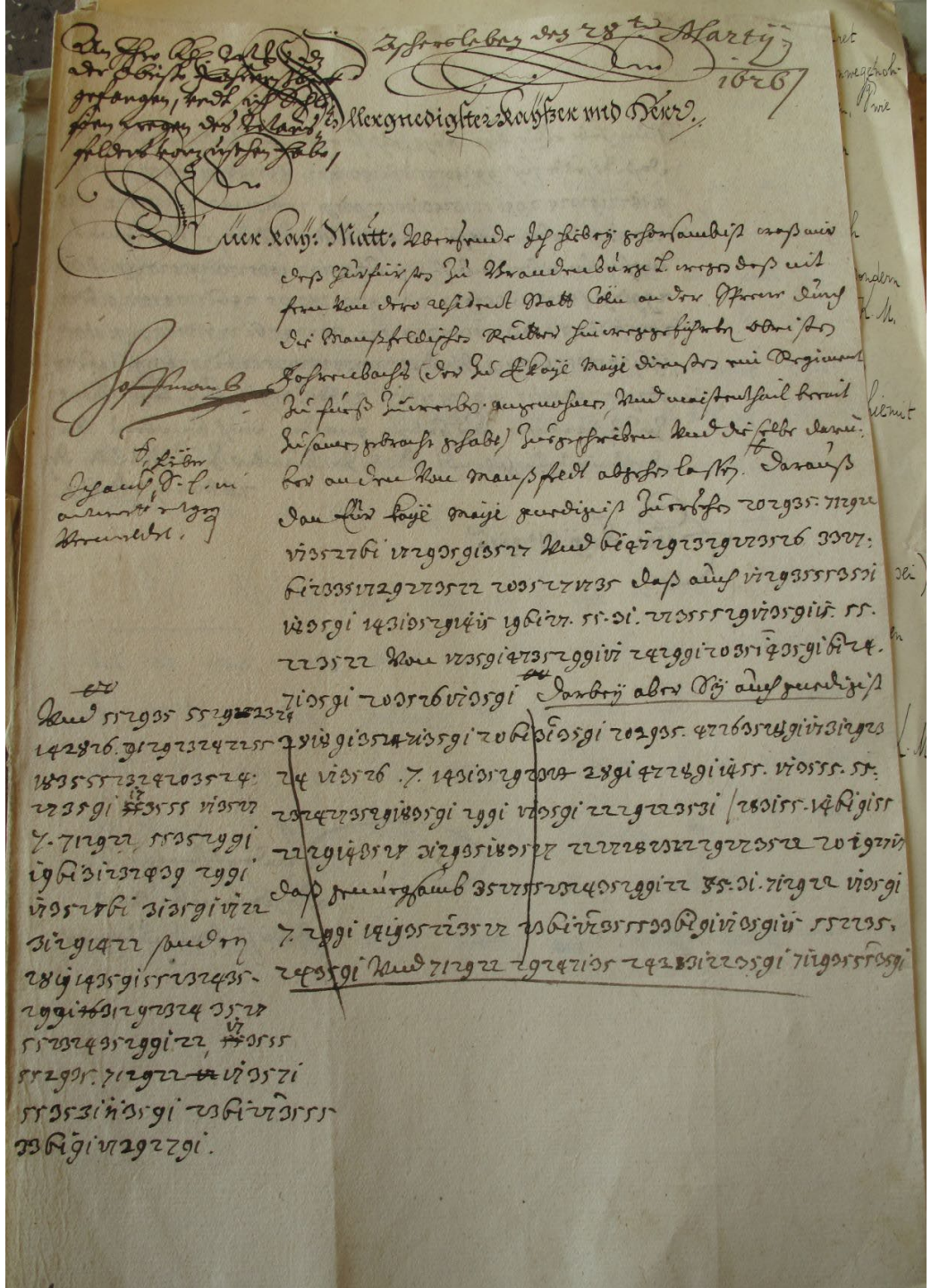
- Ucelený rozbor a přehled šifrované korespondence publikoval František Roubík. Kromě jednoho dopisu jsou všechny dešifrovány a obvykle i přepsány do otevřeného textu.

(ROUBÍK, František. Šifrované dopisy v registratuře Albrechta z Valdštejna. In: *Sborník prací věnovaných prof. Dru Gustavu Friedrichovi k šedesátým narozeninám, 1871–1931*. Praha : Historický spolek v Praze 1931, s. 359–368.)

- Fr. Roubík upozorňoval, že z cca 25 000 dopisů je jen 65 šifrovaných. Domníval se, že většina šifrovaných dopisů se musela ztratit. Tento předpoklad podporuje i fakt, že se dochovaly šifrované dopisy pouze z let 1625–1626, což je velice překvapivé.
- Nejčastějšími odesilateli a adresáty šifrovaných dopisů z těchto let jsou polní maršál Jan Tserclaes Tilly, Maxmilián Bavorský nebo císař Ferdinand II.
- Česky psané šifrované dopisy se zde nenacházejí, obvykle jsou psány německy.

Korigovaný čistopis dopisu Albrechta z Valdštejna císaři, 28. 3. 1626, Aschersleben

(Národní archiv, Valdštejniana, Jičín, inv. č. 16884)



Zachycené dopisy Karla Rabenhaupta ze Suché

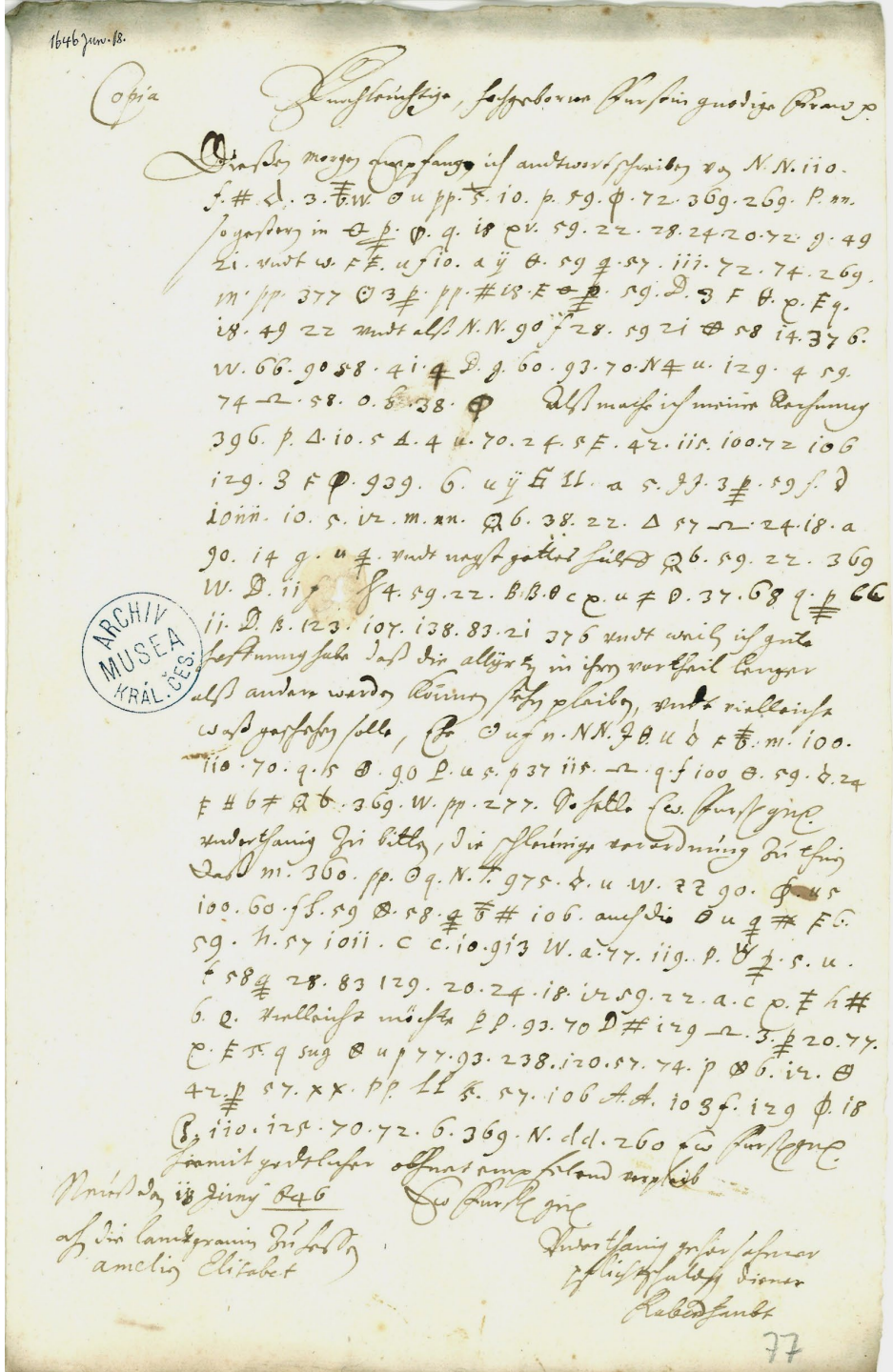
- Kopie dvou dopisů (šifrovaného a nešifrovaného) se nacházejí v písemné pozůstalosti Maxmiliána z Trauttmansdorffu. (SOA v Plzni, Rodinný archiv Trauttmansdorffů, inv. č. 125).
- Oba dopisy z července 1646 byly adresovány hessensko-kasselské lankraběnce Amálii Alžbětě a odeslány českým exulantem Karlem Rabenhauptem ze Suché, který působil v jejích službách.
- Byly zachyceny katolickou stranou u Arnsbergu a předány generálovi Alexandrovi de Bournonville. Tomu se je nepodařilo rozluštit, a tak zaslal jejich kopie Maxmiliánovi z Trauttmansdorffu, císařskému vyslanci na jednáních v Münsteru, aby se od někoho pokusil získat klíč.
- Dopisy nejsou dešifrovány, a tak byly vybrány pro kryptologickou soutěž v časopise Crypto-World. Žádný z luštitelů neuspěl. Později je zveřejnil na svém blogu také známý popularizátor kryptologie Klaus Schmeh. Ani zde nikdo neuspěl, ale jeden z přispěvatelů upozornil na možnost pátrat po souvisejících archiváliích v Hesenském státním archivu v Marburgu. Tam se opravdu podařilo Eugenovi Antalovi objevit klíč ke korespondenci.

Literatura:

ANTAL, Eugen – ZAJAC, Pavol – MÍRKA, Jakub. Solving a Mystery From the Thirty Years' War. Karel Rabenhaupt ze Suché's Encrypted Letter to Landgravine Amalie Elisabeth. In: HistoCrypt 2021 Proceedings of the 4th International Conference on Historical Cryptology, Linköping 2021, s. 12–24 (zde též odkazy na všechny předcházející práce).

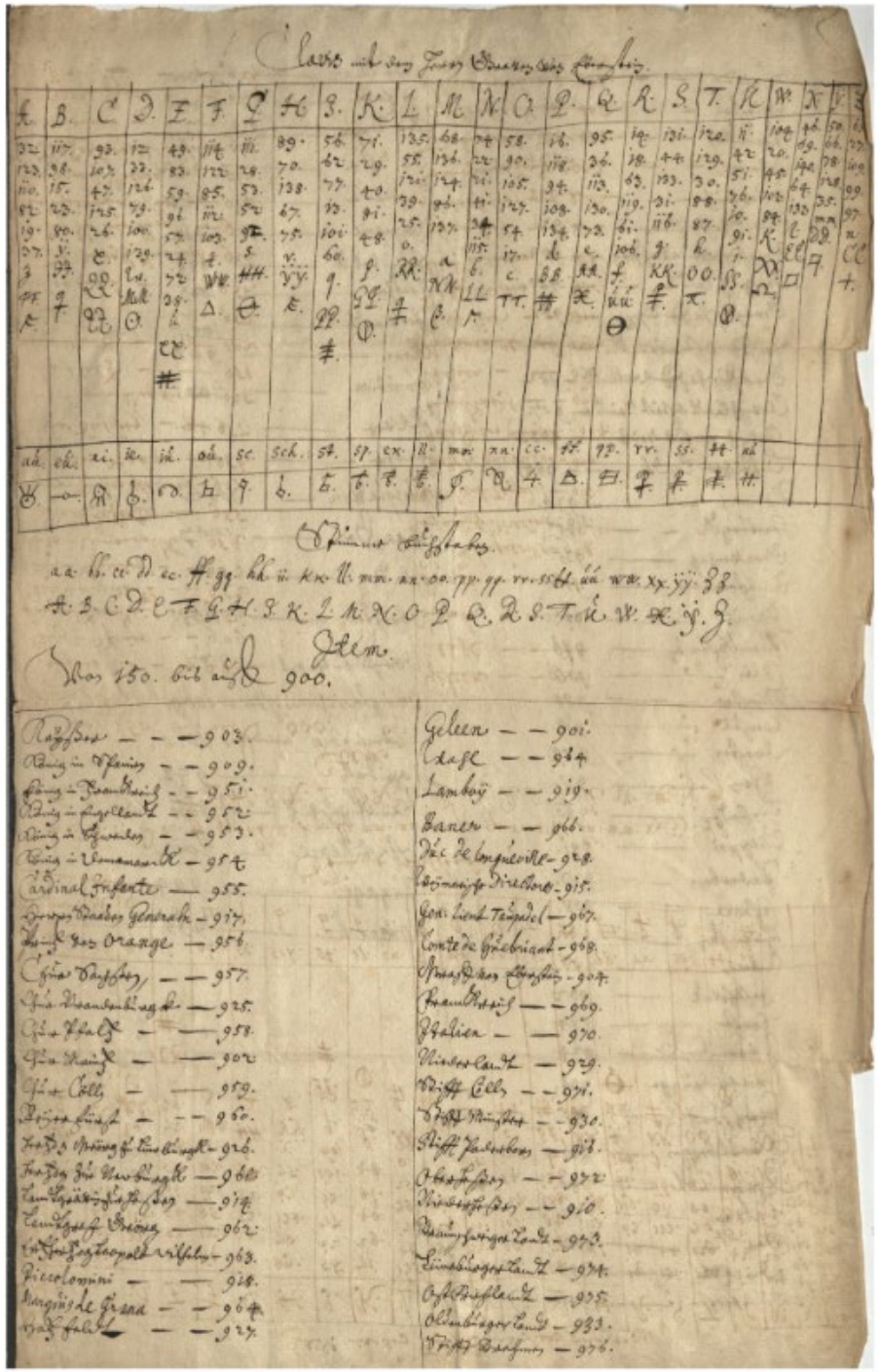
Kopie šifrovaného dopisu Karla Rabenhaupta ze Suché, datovaný 11./13. června 1646 (správně má být asi červenec)

(Státní oblastní archiv v Plzni, Rodinný archiv Trauttmansdorffů, inv. č. 125)



Klíč (nomenklátor) ke korespondenci Karla Rabenhupta ze Suché s lankraběnkou Amálií Alžbětou

(převzato z: ANTAL, Eugen – ZAJAC, Pavol – MÍRKA, Jakub. Solving a Mystery From the Thirty Years' War. Karel Rabenhaupt ze Suché's Encrypted Letter to Landgravine Amalie Elisabeth. In: HistoCrypt 2021 Proceedings of the 4th International Conference on Historical Cryptology, Linköping 2021, s. 23.)



Karel Rabenhaupt ze Suché

Karel Rabenhaupt ze Suché (1604–1675)

- Po bitvě na Bílé Hoře odešel do exilu.
- Studoval stavitelství pevností na univerzitě v Leidenu a sloužil v nizozemské armádě.
- Později vstoupil do služeb Hesensko-Kasselských lankrabat, kde se postupně vypracoval až na druhého nejvýznamnějšího vojenského velitele. Bojoval především na levém břehu Rýna.
- 1668 vystoupil ze služeb a usadil se na svých statcích v Nizozemí.
- 1672 přepadla Francie Nizozemí a Rabenhaupt se stal nizozemským národním hrdinou, protože se významně zasloužil o ubránění Groningenu a znovudobytí důležité pevnosti Coevorden, v níž se stal velitelem. Tyto činy Francii významnou měrou zabránily v rychlém dobytí Nizozemí.

Literatura:

ENGELBRECHT, Wilken. Flüchtling im fremden Lande. Weissenberger Exulanten in niederländischen Quellen. In. Sborník příspěvků IV. setkání genealogů a heraldiků. Ostrava 14.–15. 10. 1989. Ostrava 1992, s. 13–18.

ANTAL, Eugen – ZAJAC, Pavol – MÍRKA, Jakub. Solving a Mystery From the Thirty Years' War. Karel Rabenhaupt ze Suché's Encrypted Letter to Landgravine Amalie Elisabeth. In: HistoCrypt 2021 Proceedings of the 4th International Conference on Historical Cryptology, Linköping 2021, s. 12–14.

(Zdroj reprodukce: Wikipedia Commons, 2022)

Střípky z historie české kryptologie 19. století

- Šifrované deníky Karla Hynka Máchy

Analýza Máchova šifrového systému viz VONDRUŠKA, Pavel. Pár poznámek k šifře použité v deníku Karla Hynka Máchy. Crypto-World 2/2011, s. 12–20 /zde též odkazy na starší práce/.

- Úspěšné vyluštění jednoho z dopisů z let 1608–1611 uveřejněných Václavem Hankou

MALOCH, Antonín V. Rozluštění chiffrovaného písma v češtině. *Lumír* 1858, s. 205–206.

Šifrové systémy a jejich historický vývoj

Vybraná literatura:

KAHN, David. *The Codebreakers. The Story of Secret Writing*. New York: Macmillan 1967;

SINGH, Simon. *Kniha kódů a šifer.* Praha: Dokořán a Argo 2003;

JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti.* Praha: Naše vojsko, 1994;

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros 2006.

KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu.* Praha : Univerzita Karlova 1993, s. 177–209.

Pro stručný přehled dalších prací viz:

MÍRKA, Jakub. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni. *Západočeské archivy 2012*, s. 44–73. Publikováno též v Crypto-World 11, 12/2012, 1,2/2013 a 3, 4/2013 (dostupné z: http://crypto-world.info).

DĚKUJI ZA POZORNOST