Selected encrypted messages found in Slovak and Czech archives

Eugen Antal[1], Jakub Mírka [2]

[1]Institute of Computer Science and Mathematics
Slovak University of Technology
eugen.antal@stuba.sk

[2]The State Regional Archives in Pilsen
mirka@soaplzen.cz

International Conference on Historical Cryptology, Uppsala 2018

[1]This work was partially supported by grant VEGA 1/0159/17.

Outline

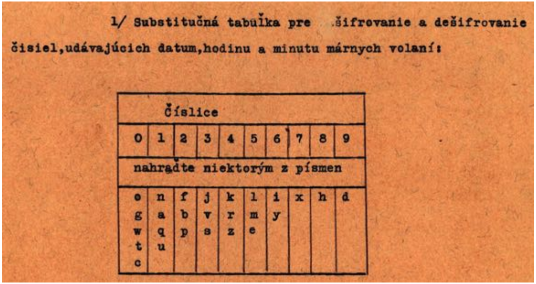
1. Encrypted correspondence
    - Archives in SK and CZ
    - Cryptogram examples
2. Research in an archive - problems and experiences
    - Searching for encrypted messages
    - Inventory
    - Digitalisation
    - OCR
    - Cryptanalysis
    - Wrong cipher designs

Archives in SK and CZ

- Looking for historical documents
  1. internet
  2. archives, libraries
- Selected historical archives from SK
  - **Slovak National Archive** (SNA) - is the largest and most significant public archive in the Slovak Republic.
  - **Institute of Military History** (IMH) - is a research and scientific, archiving and museum institution of The Ministry of Defence of the Slovak Republic in charge of military history.
- Selected historical archives from CZ
  - **National Archives** (in Prague)
  - **state regional archives** (totally 7 - e. g. State Regional Archives in Pilsen, State Regional Archives in Trebon and others)
  - **specialised archives** (e. g. The Archives of The National Museum)

Archives in SK and CZ

- Encrypted keys from WWII - IMH SK.



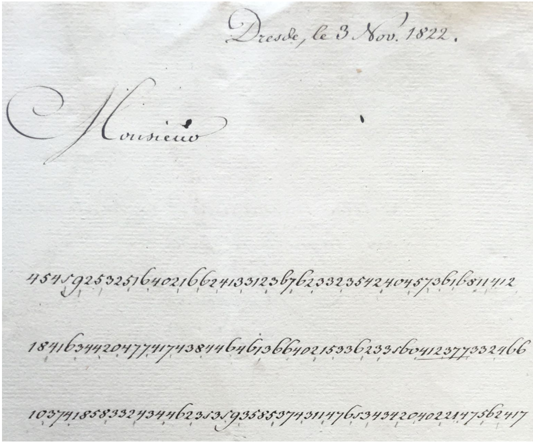
1/ Substitučná tabuľka pre šifrovanie a dešifrovanie čisiel,udávajúcich datum,hodinu a minutu márnych volaní:

Číslice									
0	1	2	3	4	5	6	7	8	9
nahraďte niektorým z písmen									
o g w t c	n a q u	f b p	j v s	k r z	l m e	i y	x	h	d

Figure: Institute of Military History. HVV. Archival fond number 29506. Box num. 89, ref. num. 213405. December 1939.

- Encrypted messages, keys from early period - regional and state archives, mostly in aristocratic family archives.

SK example - French, only code, divided



Dresde, le 3 Nov. 1822.

Monsieur

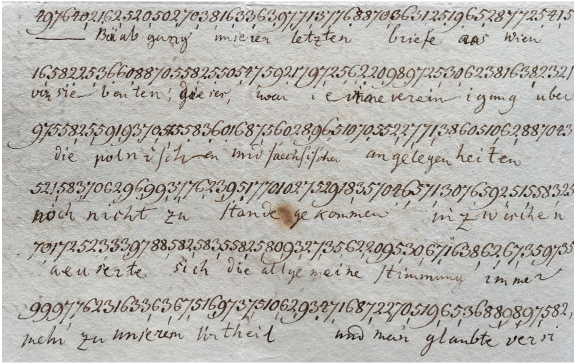
4545925325164021662413312367623323542404573616811412

1841634420477741743844646136664021533623356041237733 2466

1037418583324344623535935853743114765343420402214756 2417

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Amade-Uchtritz. Box num. 136. inv. num. 2943-2948. From November 1882.

SK example - German, code with solution, divided



4976402162520502703816336397713776887086631251965287725415
Bäab gang unſerer letzten briefe aus Wien

1658225366088705582550547592179725622098972530623816382321
vn ſie benten; gäeier, wan i e[illegible] verein igung über

9755825591937055583601687560289651070552277138605106288704
die polniſchen und ſaechſiſchen angelegenheiten

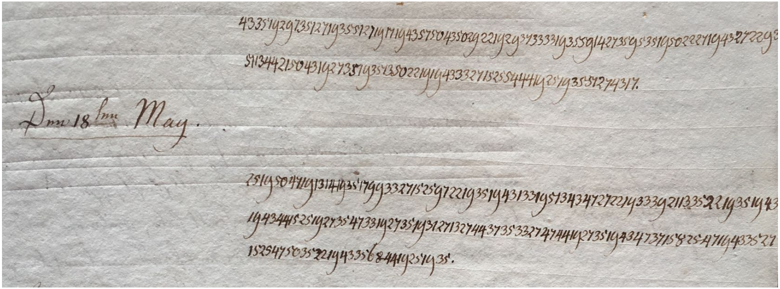
5215837062969937762395177010275291835702657130765925155832
noch nicht zu ſtande gekommen in zwiſchen

7017252333978858258355825809327356220953067163862673597 35
aeuſerte ſich die allgemeine ſtimmung immer

9997762316336367516973751062934716872270519653688989758 2,
mehr zu unſerem Vortheil und man glaubte verſi

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Amade-Uchtritz. Box num. 136, inv. num. 2906.

SK example - only code, not divided



43351929735727193557271917194357504350292219293473333193559142735953519502227194327229

5713442150431927357193573502219194333271525544419251935572743 17.

Die 18ma May.

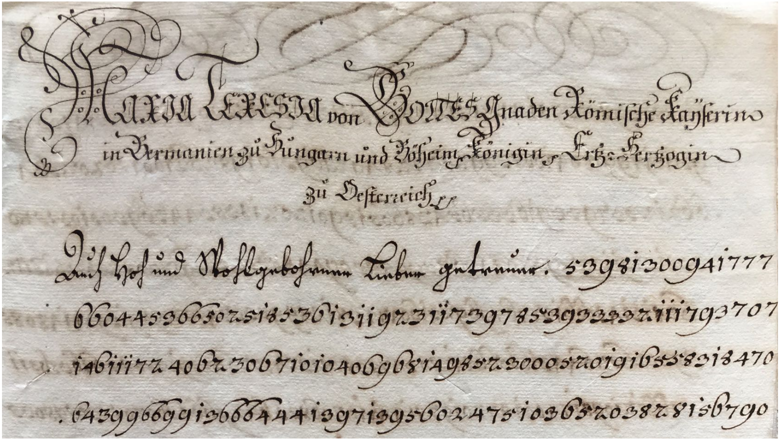
25195047191314193517993327152597221935194313319571343472722193339211335221935194

19434415251927354733192735193127132744373533274744419273519434737158254719433527

1525475035221943356844419251935.

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Amade-Uchtritz. Box num. 150, inv. num. 3144.

SK example - German, code and text, not divided

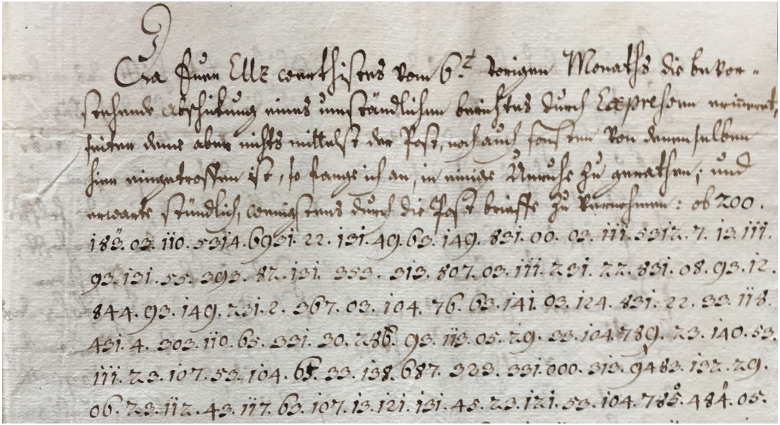


Maria Thereſia von Gottes Gnaden Römiſche Kayſerin
in Germanien zu Hungarn und Böheim Königin, Ertz-Hertzogin
zu Oeſterreich etc.

Dich hoch und Wohlgebohrnen Lieber getreuer. 53981300941777
6604453665072518553613119723117397853993332111793707
14611177240623067101040696814985230005201916558318470
.64399669913666444139713956024751036520382815 67 90

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Esterhasy, Cesnek line. Box num. 634, inv. num. 1612.

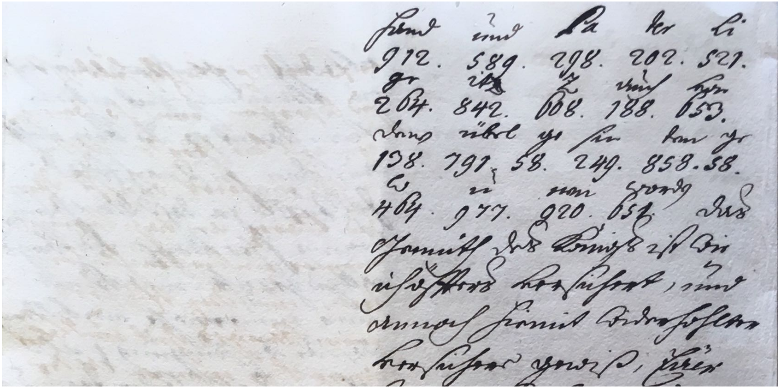
SK example - German, code and text, divided



Da Ihro Ellz confirmirend vom 6.ᵗ vorigen Monaths die bevor-
ſtehende abſchickung eines umſtändlichen berichtes durch Expreſsen erwartet,
hätten diese aber nichts mittelſt der Poſt, noch auch ſonſt ein von denenſelben
hier eingetroffen iſt, ſo fange ich an, in einige Unruhe zu gerathen; und
erwarte ſtündlich, wenigſtens durch die Poſt briefe zu vernehmen: ob 200.
182. 03. 110. 5314. 6931. 22. 131. 49. 63. 149. 831. 00. 03. 111. 5312. 7. 13. 111.
93. 131. 55. 393. 87. 131. 353. 313. 807. 03. 111. 231. 22. 831. 08. 93. 12.
844. 93. 149. 231. 2. 367. 03. 104. 76. 63. 141. 03. 124. 431. 22. 33. 118.
431. 4. 303. 110. 65. 331. 30. 286. 93. 113. 05. 29. 33. 104. 789. 23. 140. 53.
111. 23. 107. 53. 104. 65. 33. 138. 687. 323. 331. 000. 313. 9483. 132. 29.
06. 23. 112. 43. 117. 63. 107. 13. 121. 131. 45. 23. 121. 53. 104. 785. 484. 05.

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Esterhasy, Cesnek line. Box num. 634, inv. num. 1612. From May 1756.

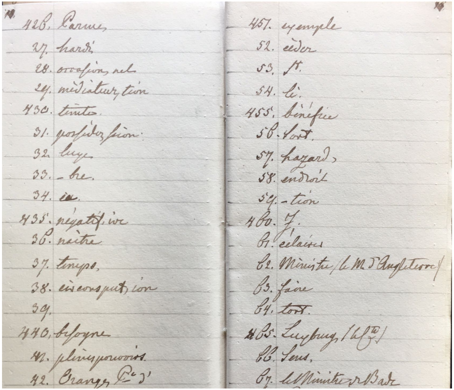
SK example - draft, code under plain-text, divided



ſend und ba ker li
912. 589. 298. 202. 521.
gr itz z uns hen
264. 842. 608. 188. 653.
dass übel ge ſin ken ge
138. 791. 58. 249. 858. 58.
w u nen gends
464. 977. 920. 657. das
Gemüth des Königs ist die
[illegible] hergeſtellt, und
demnach ſomit [illegible]
[illegible] [illegible], [illegible]

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Esterhasy, Cesnek line. Box num. 635, inv. num. 1618.

SK example - codebook

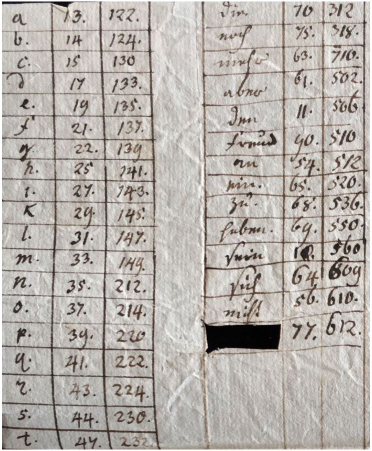


426.	Carmes,
27.	hardi,
28.	occaſion, nel
29.	médiateur, tion
430.	tentes.
31.	poſſeder, ſsion.
32.	luxe
33.	_ bre.
34.	ia.
435.	négatif, ive
36.	naître
37.	temps,
38.	circonspect, ion
39.	
440.	beſogne
41.	pleinspouvoirs.
42.	Orange, Pce d'

451.	exemple
52.	céder
53.	ſt.
54.	li.
455.	bénéfice
56.	sort.
57.	hazard,
58.	endroit
59.	- tion
460.	J.
61.	éclairer
62.	Ministre (le M. d'Angleterre)
63.	faire
64.	tort.
465.	Luxbourg, (le Pce)
66.	Sens,
67.	le Ministre de Bade

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Amade-Uchtritz. Box num. 138, inv. num. 3008.

SK example - key, "two columns/keys", missing word



a	13.	122.
b.	14	124.
c.	15	130
d	17	133.
e.	19	135.
f	21.	137.
g.	22.	139
h.	25	141.
i.	27.	143.
k	29.	145.
l.	31.	147.
m.	33.	149.
n.	35.	212.
o.	37.	214.
p.	39.	220
q.	41.	222.
r.	43.	224.
s.	44.	230.
t.	47.	232.

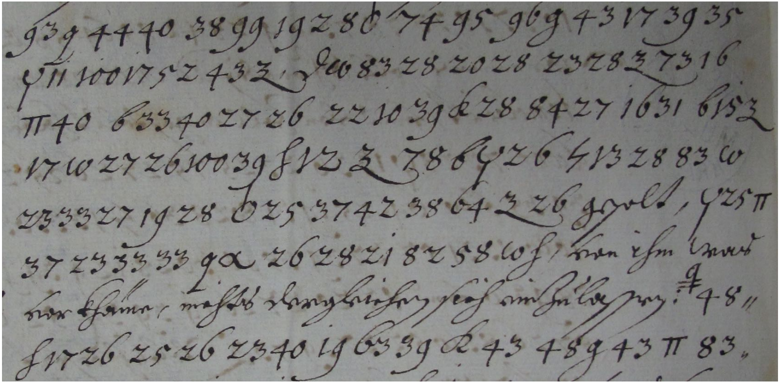
din.	70	312
noſ	75.	318.
nrſo	63.	710.
abno	61.	502.
dmn	11.	506
fornud	90.	510
an	54.	512
pin.	65.	520.
zu.	68.	536.
ſubm.	69.	550.
ſuin	10.	560
viſ	64	609
miſſ	56.	610.
	77.	612.

Figure: Ministry of Interior of the Slovak Republic. Slovak National Archive. Family Archive Amade-Uchtritz. Box num. 151, inv. num. 3146.

SK examples - summary

- Encrypted text - hundreds of pages.
- Different languages: French, German ...
- Solved and unsolved, existing keys, key reconstruction.
- Numbers - Codes and Nomenclators:
  - codes divided with **dots**;
  - some times with commas;
  - in most cases codes without division.
- Encrypted parts:
  - combined with not-encrypted;
  - only encrypted.
- Keys and codebooks:
  - One homophonic key with few codes (two lines);
  - Two codebooks - approx. 70 pages.

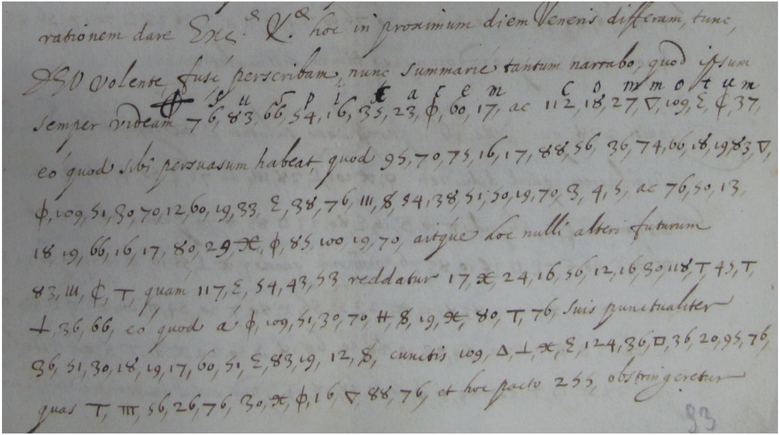
CZ example - nomenclature and text, not divided



939 4440 3899 19z8δ 7495 969 4317 3935
ϙ11 10017 5z 43ʒ, 9ω 83 z8 z0z8 z3z8ʒ 7316
π40 6334 0z7z6 zz10 39ℓ z8 84z7 1631 615ʒ
17ω z7z6 100 39 ʃ1z ʒ z8 6ϙ z6 413 z8 83 ω
z333z7 19 z8 σz5 374z 38 64ʒ z6 gewest, ϙ25π
37 z333 33 9α z6 z8 z1 8z 58 ωʃ, wen ihm unverd
[illegible] schame, machte [illegible] [illegible] um hilfe [illegible]: 9 48,,
ʃ17z6 z5 z6 z340 19 6339 ℛ 43 489 43 π 83,

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Trauttmansdorff. Box num. 9, inv. num. 200. From January 1639.

CZ example - nomenclature and text, decrypted parts, divided



rationem dare Exc.^{ae} V.^{ae} hoc in proximum diem Veneris differam, tunc

JSV volente fuse perscribam, nunc summarie tantum narrabo, quod ipsum

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

semper videam ⊕ 76, 83, 66, 54, 16, 35, 23, ϕ, 60, 17, ac 112, 18, 27, ∇, 109, Ɛ, ¢, 37,

eo quod sibi persuasum habeat, quod 95, 70, 75, 16, 17, 88, 56, 36, 74, 66, 18, 19, 83, ∇,

ϕ, 109, 51, 30, 70, 12, 60, 19, 33, Ɛ, 38, 76, 111, 8, 54, 38, 51, 50, 19, 70, 3, 4, 5, ac 76, 50, 13,

18, 19, 66, 16, 17, 80, 29, χ, ϕ, 85, 100, 19, 70, atque hoc nulli alteri futurum

83, 111, ¢, T, quam 117, Ɛ, 54, 43, 53 reddatur 17, χ, 24, 16, 56, 12, 16, 30, 118, T, 45, T,

⊥, 36, 66, eo quod a ϕ, 109, 51, 30, 70, #, 8, 19, χ, 80, T, 76, suis punctualiter

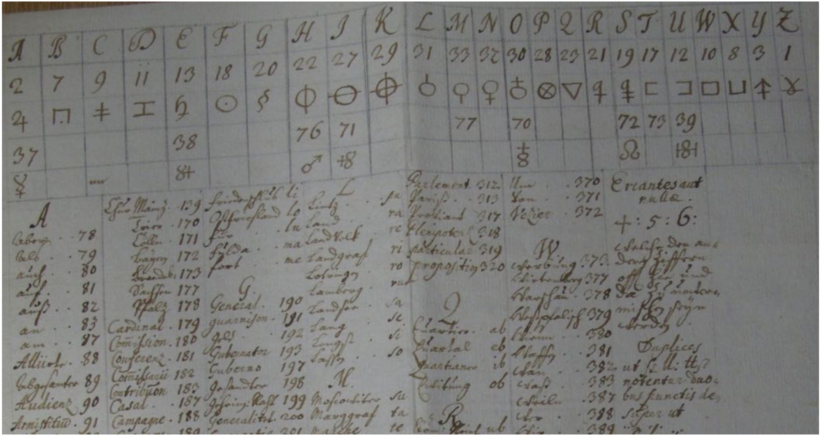
36, 51, 30, 18, 19, 17, 60, 51, Ɛ, 83, 19, 12, 8, cunctis 109, Δ, ⊥, χ, Ɛ, 124, 36, □, 36, 20, 95, 76,

quas T, ⲡ, 56, 26, 76, 30, χ, ϕ, 16, ∇, 88, 76, et hoc pacto 255, obstringeretur

93

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Trauttmansdorff. Box num. 10, inv. num. 209. From December 1645.

Nomenclature key example (codes, homophones and nulls)



A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
2	7	9	ii	13	18	20	22	27	29	31	33	32	30	28	23	21	19	17	12	10	8	3	1
4	⊓	ǂ	⌶	♄	⊙	§	ɸ	⊖	⊕	ȯ	♀	♀	♁	⊗	▽	ꝗ	ꝙ	⊏	⊐	□	⊔	↟	ɤ
37				38			76	71			77		70				72	73	39				
☿		ᵚ		84			♂	+8					⚴				Ω		ǀ8ǀ				

A

Aeberg	78
Ab	79
auf	80
auf	81
auß	82
an	83
am	87
Alliirte	88
Abgesandter	89
Audienz	90
Armistitio	91

Churf. Mainz	169
Trier	170
Cölln	171
Bayern	172
Brandenb.	173
Sachsen	177
Pfalz	178
Cardinal	179
Comission	180
Conferenz	181
Comissarii	182
Contribution	183
Casal	187
Campagne	188
[illegible]	189

Friedensschluß	li
Ostfriesland	lo
Für	lu
Fulda	ma
fort	me

G

General	190
guarnison	191
geld	192
Gubernator	193
Guberno	197
Gesandter	198
Geheimb: Rath	199
Generalitaet	200
[illegible]	201

L

Linz	pa
Land	ra
Landvolck	re
Landgraf	ri
Lothringen	ro
Lamberg	ru
Landsfor	sa
Lang	se
Längst	si
Lassen	so

M

Moscowiter	su
Marggraf	ta
Marche	te

Parlement	312
Pariß	313
Protestant	317
Plenipotent.	318
particular	319
proposition	320

Q

Quartier	ab
Quartal	eb
Quartiren	ib
Quitung	ob

R

Rom: Reich	ub

Ulm	370
Von	371
Vezier	372

W

Werbung	373
Wirtenberg	377
Warschau	378
Westphalisch	379
Wien	380
Waffen	381
Wan	382
Waß	383
Weilen	387
Wer	388
Wir	389

Errantes aut
nulla.
4: 5: 6:
Welche dan auß
den Ziffern
offt ... und
da ... zu ... andern
mit ... seyn
worden.

Duplices
ut ll: tt:
notentur duo-
bus punctis de-
super ut
[illegible]

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Windischgratz. Box num. 164, inv. num. 1403.

CZ examples - summary

- Lot of encrypted texts (thousands).
- Lot of keys, nomenclatures, code books.
- Different languages: German, French, Italian, Latin, Czech ...
- Existing keys, key reconstruction, unsolved.
- Glyphs and numbers.
- Nomenclature:
    - Homophonic substitution,
    - Bigram substitutions,
    - Codes,
    - Nulls.

Research in an archive - possible problems I

1. Where to start?
   - Ask the employees.
   - Inventory - no mention of encryption - only in two cases yet.
2. The hard way:
   - Search manually.
   - Start with aristocratic family fonds/archives.
   - Which box to choose? Only guessing?
   - Correspondence with:
     - other aristocratic families,
     - diplomacy,
     - military leaders,
     - religion related.
   - Any wars related stuff (like the Thirty Years' War).

Research in an archive - possible problems II

1. Collecting the materials:
    - Identifying the encrypted parts - codes and special symbols are not problems.
    - Making transcription of both encrypted and not encrypted parts.
    - Which one is harder? :-)

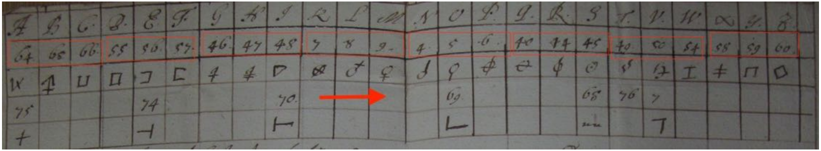
Research in an archive - possible problems II

1. Manual search is time consuming.
2. Digitalisation (recommendation - minimal 10 Mpix photos).
3. Specialised OCR (of handwriting) is needed.
4. Important tasks:
    - Identify or separate encrypted/not encrypted?
    - Specialized OCR to work only with numbers - codes.
    - Specialized OCR to work with special symbols/glyphs - nomenclature.
    - Specialized OCR to not encrypted handwritings - letters.

Research in an archive - possible problems II

1. Storing the collected data in a DB.
2. Cryptanalysis:
   - Statistical data from specific corpus (old vs. modern text).
   - Codes - identify the code-groups without separator? (2,3,4 digits and variable length)
   - Automated cryptanalysis.
3. What can also help? - Incorrect construction of codes and ciphers.
4. Some examples:

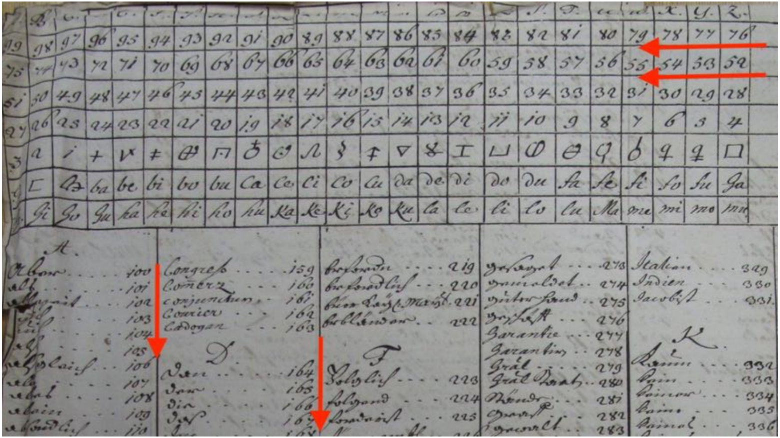
Nomenclature key, special design - increasing pattern in the homophonic key



A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	Z
64	65	66	55	56	57	46	47	48	7	8	9	4	5	6	40	44	45	49	50	54	58	59	60
1x	⊥	⊔	□	⊐	⊏	4	⋕	▷	∞	♂	♀	∫	♀	∅	[illegible]	ɸ	ʘ	[illegible]	[illegible]	I	‡	⊓	◇
75				74				70.					69.				68	76	7				
+				⊣				⊢					∟				[illegible]		˥				

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Windischgratz. Box num. 164, inv. num. 1403.

Nomenclature key, wrong design (both codes and homophonic)



[illegible]	B.	C.	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	S.	T.	u	w	X.	Y.	Z.
99	98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76
75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52
51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28
27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
3	a	i	+	Vˣ	≠	[illegible]	⊓	♁	[illegible]	∧	§	‡	▽	8	I	⊔	Φ	θ	q	6	4	4	□
[illegible]	⊏	Bz	ba	be	bi	bo	bu	Ca	Ce	Ci	Co	Cu	Da	De	Di	Do	Du	Fa	Fe	Fi	Fo	Fu	Ga
[illegible]	Gi	Go	Gu	ha	he	hi	ho	hu	Ka	Ke	Ki	Ko	Ku	la	le	li	lo	lu	Ma	me	mi	mo	mu

A.

Albion	100
alß	101
[illegible]	102
[illegible]	103
[illegible]	104
[illegible]	105
[illegible]	106
[illegible]	107
[illegible]	108
[illegible]	109
[illegible]	110
Congreß	159
Comerz	160
conjunctum	161
Courier	162
Cadogan	163

D.

Dan	164
Dom	165
Dir	166
Dies	167
Erfordern	219
erforderlich	220
Erb Landt Marsch.	221
Erblanden	222

F

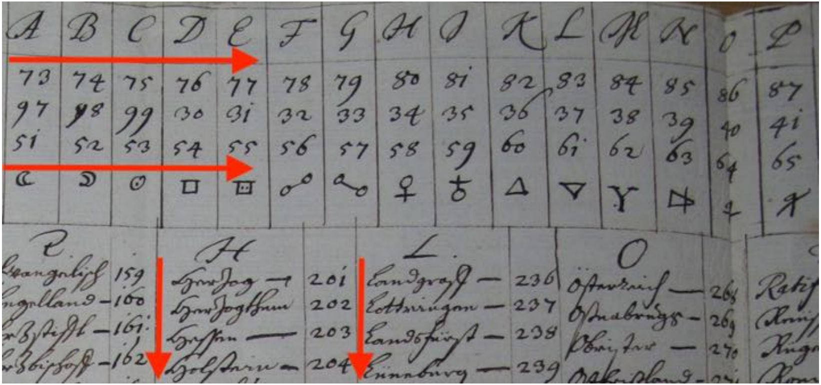
Folglich	223
folgend	224
fordersamst	225
gefangen	273
gemeldet	274
guter Freund	275
gesetzt	276
Garantie	277
Garantirn	278
Graf	279
Graf Staats	280
Gränitz	281
[illegible]	282
General	283
Italien	329
Indien	330
Jacobit	331

K.

[illegible]	332
[illegible]	333
[illegible]	334
[illegible]	335
[illegible]	336

Figure: State Regional Archives in Pilsen, workplace Klaster Family Archive Windischgratz. Box num. 164, inv. num. 1403.

Nomenclature key, wrong design (both codes and homophonic)

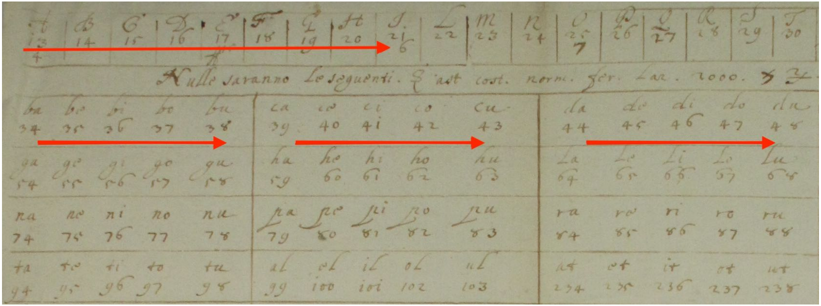


A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
73	74	75	76	77	78	79	80	81	82	83	84	85	86	87
97	98	99	30	31	32	33	34	35	36	37	38	39	40	41
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
☾	☽	☉	□	⊡	☍	☊	♀	♄	△	▽	♈	⊐	♃	♂

E.		H		L.		O		
Evangeliſch	159	Herzog —	201	Landgraff —	236	Oeſterreich —	268	Ratiſ
Engelland —	160	Herzogthum	202	Lothringen —	237	Oſnabrügg —	269	Kron
Erzſtifft —	161	Heſſen —	203	Landsfürſt —	238	Obriſter —	270	Krieg
Erzbiſchoff —	162	Holſtein —	204	Lünnburg —	239	Oſtfrieſland —	27	Rom

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Windischgratz. Box num. 164, inv. num. 1403.

Nomenclature key, wrong design (both 2-grams and substitution)



A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T
13 4	14	15	16	17	18	19	20	21 6	22	23	24	25 7	26	27	28	29	30

Nulle saranno le seguenti. & ast cost. norm. fer. Lar. 2000.

ba 34	be 35	bi 36	bo 37	bu 38	ca 39	ce 40	ci 41	co 42	cu 43	da 44	de 45	di 46	do 47	du 48
ga 54	ge 55	gi 56	go 57	gu 58	ha 59	he 60	hi 61	ho 62	hu 63	La 64	Le 65	Li 66	Lo 67	Lu 68
na 74	ne 75	ni 76	no 77	nu 78	pa 79	pe 80	pi 81	po 82	pu 83	ra 84	re 85	ri 86	ro 87	ru 88
ta 94	te 95	ti 96	to 97	tu 98	al 99	el 100	il 101	ol 102	ul 103	at 234	et 235	it 236	ot 237	ut 238

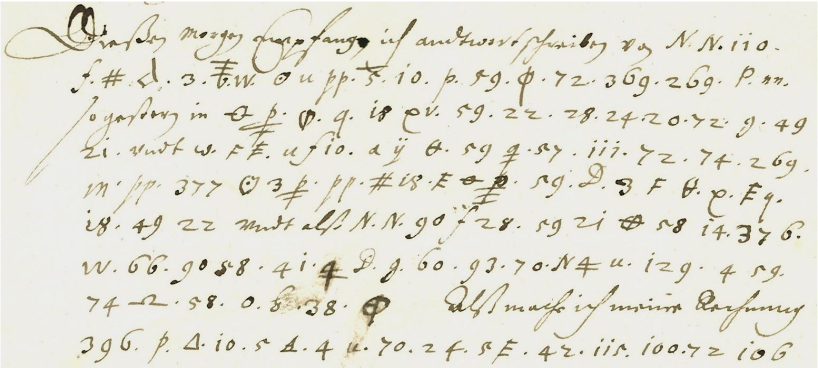
Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Windischgratz. Box num. 164, inv. num. 1403.

Q & A?

Challenge - Unsolved encrypted message

- Carl von Rabenhaupt sent to Amalie Elisabeth Landgrave von Hessen.
- Never received - never decrypted!
- Nomenclature (576 symbols, 80 unique).
- Challenge published by Jakub Mírka and Pavel Vondruška in Crypto-World 7-8/2013. ISSN 1801-2140. pp 10-18.
  Available online: `http://crypto-world.info/casop15/crypto0708_13.pdf`.
- Analysis of the cryptogram published by E. Antal and P. Zajac: in Crypto-World 11-12/2013. ISSN 1801-2140. pp 9 -17.
  Available online: `http://crypto-world.info/casop15/crypto1112_13.pdf`.

Challenge - Unsolved encrypted message



Dieſen morgen empfangen ich antwortſchreiben von N.N. 110.
f.#.d.3.ŧw. ⊙ u pp.ŧ.10. p.59.φ.72.369.269. P.nn.
ſo geſtern in ⊖ ꝑ. φ. q. i8 ev. 59.22.28.24.20.72. g.49
21. undt w. F Ŧ. u f io. a ÿ θ. 59 ǂ.57. iii.72.74.269.
m' pp. 377 ⊙ 3 ꝑ. pp.# i8. E ⊖ ꝑ. 59. D. 3 F θ. e. F9.
i8. 49 22 undt alſ N.N. 90 f 28. 59 21 ⊖ 58 14.376.
w. 66. 90 58. 4i. ǂ D. g. 60. 93.70. N ǂ u. 129. 4 59.
74 Ω. 58. 0.8.38. φ alſ mache ich meine rechnung
396. p. Δ.10.5 Δ.4 u.70.24.5E.42.iir.100.72 106

Figure: State Regional Archives in Pilsen, workplace Klaster. Family Archive Trauttmansdorff. Inv. num. 125. From 1646.