Classical Cryptography

Transposition cryptanalysis

Karst Koymans

Informatics Institute

University of Amsterdam

(version 22.4, 2023/02/20 11:48:28 UTC)

Tuesday, February 21, 2023

1. Keyed columnar transpositions
   - Completely filled rectangles
   - Partly filled rectangles
2. Multiple anagramming

Outline

Outline

Determine rectangle width

- Guess a width (a divisor of the length) and fill in the rectangle as if it was a simple columnar transposition
- Look at the distribution of vowels and consonants over the rows
- In the English language 38% of letters is a vowel
- For N random choices out of this vowel distribution
  - The expected number of vowels is $0.38 \cdot N$
  - The expected variance is $0.38 \cdot 0.62 \cdot N$
- For N letters from English texts the variance should be lower

Math of Secrets: 3.6 transposition

OHIVR SVAHT BLRHL HLBIT MBETM NOEIO

ITETK ROWTN ATHIG NSDEN UPBLN TSEMA

TADAA ERARI AOWSA YIAPT NAEOW BCDRE

WAHMT GEDER HFDDT EAEHA TEHME IELBO

HIUSI EKIUE UHESL MTKSE CREP

Calculate the variance of number of vowels for all the possible rectangles you can form from this block of 144 letters.

Assume that the minimum width or length is 4.

Anagramming

- After determination of the rectangle shape one can start anagramming the columns
- Look for probable digraphs for two columns
- Use the **contact method** for the most probable choice(s)
- Therefore find and add the **log weights** for the options
- The closer this sum of logarithms of digraph frequencies is to zero,

  the more probable the option is

An Italian military example

RIOQK DEEFG ATCIE EGNEE NRMEN

NTOAV PTINT BAALL IUSUR OSNOE

NACGC YZATA MLALR ROKOI IA

Completely filled columns

Adapted from slides by Hans van der Meer

Filled columns

1. Find the size of the transposition block

As an example take 72 letters

```
1  block of size 72: 2x36 3x24 4x18 6x12 8x9
2 blocks of size 36: 2x18 3x12 4x9 6x6
3 blocks of size 24: 2x12 3x8 4x6
```

2. Divide the cryptogram in columns

3. Anagram these columns

Example

Italian military message with

72 letters in one block

```
RIOQK DEEFG ATCIE EGNEE NRMEN
NTOAV PTINT BAALL IUSUR OSNOE
NACGC YZATA MLALR ROKOI IA
```

How many columns?

Use vowel distribution

2 RCNAOM		
4 IINAEL		
3 OETLNA		
3 QEOLAL	4 RGEOAOCL	
2 KGAICR	5 IAEAASVR	3 RFGNIIOZR
1 DNVUGR	1 OTNVLNZR	4 IGNNNUEAR
2 EEPSCC	3 QCRPLOAO	4 OAETTSNTO
3 EETUVK	3 KIMTIETK	5 QTEOBUAAK
2 FNIRZO	6 DEEIUNAO	3 KCNAARCMO
3 GRNOAI	4 EENNSAMI	4 DIRVAOGLI
2 AMTSTI	3 EGNTUCLI	4 EEMPLSCAI
3 TEBNAA	2 FNTBRGAA	4 EEETLNVLA
12X6	9X8	8X9

Anagramming

Special combination of Q and U

123456789	2345789 16
RFGNIIOZR	FGNIOZR RI
IGNNNUEAR	GNNNEAR IU
OAETTSNTO	AETTNTO OS
QTEOBUAAK	TEOBAAK QU
KCNAARCMO	CNAACMO KR
DIRVAOGLI	IRVAGLI DO
EEMPLSCAI	EMPLCAI ES
EEETLNVLA	EETLVLA EN

Find good third column

4 options

2345789	16	163	164	167	168
FGNIOZR	RI	RIG	RIN	RIO	RIZ
GNNNEAR	IU	IUN	IUN	IUE	IUA
AETTNTO	OS	OSE	OST	OSN	OST
TEOBAAK	QU	QUE	QUO	QUA	QUA
CNAACMO	KR	KRN	KRA	KRC	KRM
IRVAGLI	DO	DOR	DOV	DOG	DOL
EMPLCAI	ES	ESM	ESP	ESC	ESA
EETLVLA	EN	ENE	ENT	ENV	ENL

Use a digram count

2345789	16	163		164		167		168	
FGNIOZR	RI	RIG	40	RIN	114	RIO	110	RIZ	5
GNNNEAR	IU	IUN	46	IUN	46	IUE	40	IUA	35
AETTNTO	OS	OSE	91	OST	94	OSN	0	OST	94
TEOBAAK	QU	QUE		QUO		QUA		QUA	
CNAACMO	KR	KRN	16	KRA	124	KRC	24	KRM	16
IRVAGLI	DO	DOR	108	DOV	42	DOG	19	DOL	81
EMPLCAI	ES	ESM	11	ESP	16	ESC	35	ESA	30
EETLVLA	EN	ENE	110	ENT	124	ENV	5	ENL	3

A nice fourth column

235789	164	1642		1645		1649	
FGIOZR	RIN	RINF	5	RINI	54	RINR	0
GNNEAR	IUN	IUNG	13	IUNN	24	IUNR	0
AETNTO	OST	OSTA	21	OSTT	56	OSTO	113
TEBAAK	QUO	QUOT	30	QUOB	8	QUOK	0
CNACMO	KRA	KRAC	54	KRAA	24	KRAO	13
IRAGLI	DOV	DOVI	38	DOVA	24	DOVI	38
EMLCAI	ESP	ESPE	67	ESPL	0	ESPI	27
EELVLA	ENT	ENTE	102	ENTL	0	ENTA	121

Remaining columns

35789 1642	35789 164279853	SOLUTION
GIOZR RINF	GIOZR RINF	RINFORZIG
NNEAR IUNG	NNEAR IUNG	IUNGERANN
ETNTO OSTA	ETNTO OSTA	OSTANOTTE
EBAAK QUOT	EBAAK QUOT	QUOTAKABE
NACMO KRAC	NACMO KRAC	KRACCOMAN
RAGLI DOVI	RAGLI DOVI	DOVIGILAR
MLCAI ESPE	MLCAI ESPECIALMENTE	ESPECIALM
ELVLA ENTE	ELVLA ENTE	ENTEVALLE

What does this final text mean?

Outline

Disrupted columnar transposition

- Using an incompletely (partly) filled rectangle
- Common start or ending of messages helps
- This can help to determine long and short columns
- Long columns to the left, short ones to the right
- Now do simultaneous anagramming on each of the three parts

Incompletely filled columns

Adapted from slides by Hans van der Meer

Partly filled block

TSURC KNLCA PTEPE TLTTN EKCOI OAODH O

		lssslsl	
		EL	
Plaintext		CPTK	
7153624	*lllssss*	CAETCA	*sssslll*
ATTACKP	TKPTNOO	TKPTNOO	TCCELKA
OSTPONE	SNTLEID	SNTLEID	SKAPTCO
DUNTILT	ULETKOH	ULETKOH	UNPETOD
HREEOCL	RCPTCAO	RCPTCAO	RLTTNIH
OCK	CAE	CAE	EOO

Identical beginning

cryptogram 1

BNTSE ARKCL CETTN BITER ROTAE LTNNO
NNENO OTOKM SZTGN YITDK LANAE FTFSN
PGNPA RWOIA OFGTF CTOTD NINOE WXERF
ASIOS TIDRR RMMAO ARPAT OUTIO BIEOA
GAAPN EIK

cryptogram 2

BNTSE INDOT LCETS AFPLE RROMO ISOEN
NONST IIUTO KMFEY KPCYI TDVSI NTAEF
TFSTO NTNAR WOARO EEKTF CTTLT AEANO
EWXPV TITIO STTTF OCMMA OOSCA NROUT
IEELS OAGAA ABITR T

Similarities

cryptogram 1

BNTSEARKC LCETTNBIT ERROTAELT
NNONNENOO TOKMSZTGN YITDKLAN
AEFTFSNPGNP ARWOIAOFG TFCTOTDNI
NOEWXERFAS IOSTIDRRR MMAOARPAT
OUTIOBIEO AGAAPNEIK

cryptogram 2

BNTSEINDOT LCETSAFPL ERROMOISOE
NNONSTIIU TOKMFEYKPC YITDVSINT
AEFTFSTONTN ARWOAROEEK TFCTTLTAEA
NOEWXPVTIT IOSTTTFOC MMAOOSCANR
OUTIEELSO AGAAABITRT

Accidental coincidences

Identical parts of this cryptogram lined up

long = short + 1
This A disturbs the pattern (accidental hit)
A belongs at the end of the line before

cryptogram 1	*cryptogram 2*
BNTSEARKC	BNTSEINDOT
LCETTNBIT	LCETSAFPL
ERROTAELT	ERROMOISOE
NNONNENOO	NNONSTIIU
TOKMSZTGN	TOKMFEYKPC
YITDKLAN	YITDVSINT
AEFTFSNPGNP	AEFTFSTONTN
ARWOIAOFG	ARWOAROEEK
TFCTOTDNI	TFCTTLTAEA
NOEWXERFAS	NOEWXPVTIT
IOSTIDRRR	IOSTTTFOC
MMAOARPAT	MMAOOSCANR
OUTIOBIEO	OUTIEELSO
AGAAPNEIK	AGAAABITRT

Permuted columns

cryptogram 1

BLENTYEATNIMOA
NCRNOIFRFOOMUG
TEROKTTWCESATA
STONMDFOTWTOIA
ETTNSKSIOXIAOP
ANAEZLNATEDRBN
RBENTAPODRRPIE
KILOGNGFNFRAEI
CTTONANGIARTOK
P S

cryptogram 2

BLENTYEATNIMOA
NCRNOIFRFOOMUG
TEROKTTWCESATA
STONMDFOTWTOIA
ESMSFVSATXTOEA
IAOTESTRLPTSEB
NFIIYIOOTVFCLI
DPSIKNNEATOAST
OLOUPTTEEICNOR
T E CANKAT R T

Long columns left

cryptogram 1

ENBLENTYATIMOA
FONCRNOIRFOMUG
TETEROKTWCSATA
FWSTONMDOTTOIA
SXETTNSKIOIAOP
NEANAEZLATDRBN
PRRBENTAODRPIE
GFKILOGNFNRAEI
NACTTONAGIRTOK
PS

cryptogram 2

BLENTYEATNIMOA
NCRNOIFRFOOMUG
TEROKTTWCESATA
STONMDFOTWTOIA
ESMSFVSATXTOEA
IAOTESTRLPTSEB
NFIIYIOOTVFCLI
DPSIKNNEATOAST
OLOUPTTEEICNOR
T E CANKAT R T

Short columns right

cryptogram 1

ENBLENTYATIMOA
FONCRNOIRFOMUG
TETEROKTWCSATA
FWSTONMDOTTOIA
SXETTNSKIOIAOP
NEANAEZLATDRBN
PRRBENTAODRPIE
GFKILOGNFNRAEI
NACTTONAGIRTOK
PS

cryptogram 2

ENBETYATMALNIO
FONROIRFMGCNOU
TETRKTWCAAEOST
FWSOMDOTOATNTI
SXEMFVATOASSTE
TPIOESRLSBATTE
OVNIYIOTCIFIFL
NTDSKNEAATTPOS
TIOOPTEENRLUCO
NTTECAKART

Three parts

Simultaneous anagramming per part
ENEMY BATTALION…

cryptogram 1

ENBETYATMALNIO
FONROIRFMGCNOU
TETRKTWCAAEOST
FWSOMDOTOATNTI
SXETSKIOAPTNIO
NEAAZLATRNNEDB
PRRETAODPEBNRI
GFKLGNFNAIIORE
NACTNAGITKTORO
PS

cryptogram 2

ENBETYATMALNIO
FONROIRFMGCNOU
TETRKTWCAAEOST
FWSOMDOTOATNTI
SXEMFVATOASSTE
TPIOESRLSBATTE
OVNIYIOTCIFIFL
NTDSKNEAATTPOS
TIOOPTEENRLUCO
NTTECAKART

The final result

cryptogram 1

ENEMYBATTALION
FORMINGFORCOUN
TERATTACKWESTO
FWOODSATMOTTIN
SXTAKEPOSITION
NEARLANTZANDBE
PREPAREDTOBRIN
GFLANKINGFIREO
NATTACKINGTROO
PS

cryptogram 2

ENEMYBATTALION
FORMINGFORCOUN
TERATTACKWESTO
FWOODSATMOTTIN
SXMOVEATFASTES
TPOSSIBLERATET
OVICINITYOFFLI
NTSANDTAKETOSP
TIONTOREPELCOU
NTERATTACK

Outline

Multiple similarly encrypted texts

S E U I S M D M N A A S

J Y I N B N D H N O A L

L L N A A U E L C U I D

J E E I P K D C N A A E

B A I Y R D B D D U N G

- Multiple messages of the same length, encrypted with the same system
- Now you can try to use **multiple anagramming**

Multiple Anagramming

Adapted from slides by Hans van der Meer

Identical transpositions

From General Calamity
to Mayor Catastrophy

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

Military terminology
Four parts with identical transposition
Simultaneous anagramming

Probable word

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

ATTACK ENEMY

1	A			T			T			A		C	K
2	P	R	S	A	U	N	A	U	N	P	R	S	I	S
3	E	C	T	A	I	N	A	I	N	E	C	T	A	S
4	P	F	R	T	E	D	T	E	D	P	F	R	O	R

1	E			N		E			M	Y
2	E	O	T	E	S	E	E	O	T	E	U	T
3	F	O	D	R	T	F	F	O	D	R	R	E
4	U	A	E	R	W	A	U	A	E	R	R	D

Simultaneous text

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

2 SUNRISE
4 REWARD

1	A			T			T			A	C	K
2	P	R	S	A	U	N	A	U	N	P	R	S	I	S
3	E	C	T	A	I	N	A	I	N	E	C	T	A	S
4	P	F	R	T	E	D	T	E	D	P	F	R	O	R

1	E			N		E			M	Y
2	E	O	T	E	S	E	E	O	T	E	U	T
3	F	O	D	R	T	F	F	O	D	R	R	E
4	U	A	E	R	W	A	U	A	E	R	R	D

Chosen letters

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

3 IN CASE OF

1	A			T			T			A			C	K
2			S		U				N		R		I	S
3			T		I				N		C		A	S
4			R		E				D		F		O	R

1	E			N		E			M	Y	
2			T		S			O			U	T
3			D		T			O			R	E
4			E		W			A			R	D

Extend

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

2 SUNRISE
3 IN CASE OF

1	A	T	T	A	C	K	S	H	E	N	
2	S	U	N	R	I	S	E	B	E	E	
3	T	I	N	C	A	S	E	O	F		
4	R	E	D	F	O	R	Y	O	U	A	

Another probable word

1	T			A				G	S	L	L	I	W		N						E	I	
2	A			P				R	P	E	M	O	C		E						E	R	
3	A			E				T	D	A	E	R	T		F						R	E	
4	T			P				U	R	E	F	F	O		A						R	C	

3 DEFEAT

1	S	A	L	I	N	A	L	I	T	L	G	W
2	P	P	M	R	E	P	M	R	A	E	R	C
3	D	E		F		E		A		T		
4	R	P	F	C	A	P	F	C	T	E	U	O

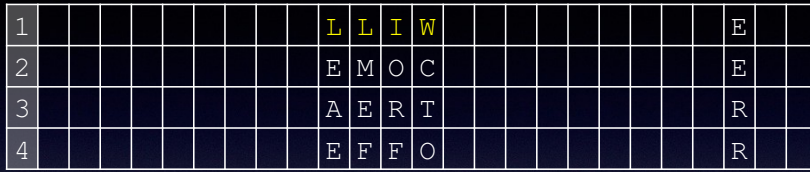
New word visible

1	T			A				G		L	L	I	W									E	I	
2	A			P				R		E	M	O	C									E	R	
3	A			E				T		A	E	R	T									R	E	
4	T			P				U		E	F	F	O									R	C	

2 PREPARE

1	S	A	L	I	N	A	L	I	T	L	G	W
2	P	P	M	R	E	P	M	R	A	E	R	C
3	D		E		F		E		A		T	
4	R	P	F	C	A	P	F	C	T	E	U	O

Fragments



ENEMY WILL ATTACK

1	E	N	E	M	Y
2	T	S	O	U	T
3	D	T	O	R	E
4	E	W	A	R	D

1	A	T	T	A	C	K	S	H	E
2	S	U	N	R	I	S	E	B	E
3	T	I	N	C	A	S	E	O	F
4	R	E	D	F	O	R	Y	O	U

1	S	I	N	A	T	G
2	P	R	E	P	A	R
3	D	E	F	E	A	T
4	R	C	A	P	T	U

Final steps

1	E	N	E	M	Y	W	I	L	L	A	T	T	A	C	K
2	T	S	O	U	T	C	O	E	M	E	M	S	U	N	R	I	S
3	D	T	O	R	E	T	R	A	E	A	E	T	I	N	C	A	S
4	E	W	A	R	D	O	F	E	F	E	F	R	E	D	F	O	R

Plaintext

E	N	E	M	Y	W	I	L	L	A	T	T	A	C	K	S	H	E	S	I	N	A	T	G	E
T	S	O	U	T	C	O	M	E	S	U	N	R	I	S	E	B	E	P	R	E	P	A	R	E
D	T	O	R	E	T	R	E	A	T	I	N	C	A	S	E	O	F	D	E	F	E	A	T	R
E	W	A	R	D	O	F	F	E	R	E	D	F	O	R	Y	O	U	R	C	A	P	T	U	R