Cursus Cryptografie

Breken polyalfabeet

gepermuteerd alfabet

21-02-2016

Onderwerpen

- alfabet matching
- symmetrie in positie
- isomorfie
- decimatie van het alfabet

Klaaralfabet gemengd

```
klaaralfabet:  LEAVNWORTHBCDFGIJKMPQSUXYZ
cijferalfabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
klaartekst:    LEAV
cijfertekst:   ABCD   sleutel = ‘L-A’

klaaralfabet:  LEAVNWORTHBCDFGIJKMPQSUXYZ
cijferalfabet: BCDEFGHIJKLMNOPQRSTUVWXYZA
klaartekst:    LEAV
cijfertekst:   BCDE   sleutel = ‘L-B’

klaaralfabet:  LEAVNWORTHBCDFGIJKMPQSUXYZ
cijferalfabet: CDEFGHIJKLMNOPQRSTUVWXYZAB
klaartekst:    LEAV
cijfertekst:   CDEF   sleutel = ‘L-C’
```

Alfabet match

```
klaartekst:     LEAV
cijfertekst:    ABCD
```

→


```
klaartekst:     LEAV
cijfertekst:    BCDE
```

→


```
klaartekst:     LEAV
cijfertekst:    CDEF
```

→

Cryptoanalyse klaaralfabet gemengd

1. bepaal periode
   (Kasiski, statistische methode)
2. voer alfabetmatching uit
3. los resulterende monoalfabeet op

Cijferalfabet gemengd

```
klaaralfabet:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
cijferalfabet: LEAVNWORTHBCDFGIJKMPQSUXYZ
klaartekst:    ABCD
cijfertekst:   LEAV    sleutel = ‘A-L’

klaaralfabet:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
cijferalfabet: EAVNWORTHBCDFGIJKMPQSUXYZL
klaartekst:    ABCD
cijfertekst:   EAVN    sleutel = ‘A-E’

klaaralfabet:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
cijferalfabet: AVNWORTHBCDFGIJKMPQSUXYZLE
klaartekst:    ABCD
cijfertekst:   AVNW    sleutel = ‘A-A’
```

Geen alfabet matching !

```
klaartekst:     ABCD
cijfertekst:    LEAV
```

→


```
klaartekst:     ABCD
cijfertekst:    EAVN
```

→


```
klaartekst:     ABCD
cijfertekst:    AVNW
```

→

Cryptoanalyse cijferalfabet gemengd

1. bepaal periode
   (Kasiski, statistische methode)
2. bepaal cijfertekst alfabet
   (symmetrie in positie, isomorfie)
3. voer alfabetmatching uit
4. los resulterende monoalfabeet op
   als klaar- & cijfertekstalfabet allebei gemengd

Tellingen per positie

	5-1-2	1-2-3	2-3-4	3-4-5	4-5-1
A	QP CT	ST NG	Y H	Z O	CKKCB IGGMI
B	GOGOGG WPKWLX	RVIMSCI ZGEJGYW	IWCWN KRYIR	NDDN QNLA	
C	NTTW TCTB	IQVCIMA JGGBGJJ		VJXFNHLDNV AIUONDAJQL	
D				GG GN	
E	T V	...	...	...	...
F		...	...	...	...
G	AALL EDXW	...	...	...	...
H		...	...	...	...
I	AWHNGWXGINAQ SCWDVCDBVRKB	...	...	...	...

Conclusies uit telling

alfabet	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G?)	I=e M=o Q=r V=t C=a/i(?)
2	WPI	BCDT	W=e
3	GZ	JNDYF	G=e(?)
4	C(ERB?)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Symmetrie in positie

pt:	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5					Q																					

alfabet	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G?)	I=e M=o Q=r V=t C=a/i(?)
2	WPI	BCDT	W=e
3	GZ	JNDYF	G=e(?)
4	C(ERB?)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Symmetrie in positie

pt:	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5		M			Q		V							C				I				C				

Q→V in 1 twee stappen dan ook Q→V in 5 twee stappen

In 5 nu ook CMI te plaatsen

Gebruik lettertelling

pt:	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5		M			Q		V							C				I				C				

Kan C worden opgelost?
C komt niet voor in 5

Waarschijnlijk C in 5 = V niet N
en dus ook C = I in 1

Symmetrie (1,5) → 4

pt:	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					I				C						M			Q		V						
2					W																					
3					G																					
4	I				C						M			Q		V										
5		M			Q		V											I				C				

Is Symmetric Encryption Broken?

pt:	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			S		I				C						M			Q	R	V						
2					W																					
3					G											B										
4	I				C						M			Q	R	V									S	
5		M			Q	R	V									S		I				C				

123451 5123451
QWBRIV SQWBIIJ
re??rt ?re?are

?

123451 5123451
QWBRIV SQWBIIJ
report prepare

Klinkers in 2

pt:	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			S		I				C						M			Q	R	V						
2	P	Q	R	V	W																					
3					G											B										
4	I				C						M			Q	R	V									S	
5		M			Q	R	V									S		I				C				

alfabet	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G?)	I=e M=o Q=r V=t C=a/i(?)
2	WPI	BCDT	P=a?
3	GZ	JNDYF	G=e(?)
4	C(ERB?)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Cijferalfabet completeren

pt:	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			S		I				C						M		P	Q	R	V	W					
2	P	Q	R	V	W								S		I				C						M	
3					G											B										
4	I				C						M		P	Q	R	V	W								S	
5		M		P	Q	R	V	W								S		I				C				

Enzovoorts

Isomorfie

- ... ABABCD ..... ABABCD *herhaling*
- ... ABABCD ..... KQKQAZ *isomorf*
  ABABCD → monoalfabetisch → KQKQAZ

- zoeken van isomorfen:
  - begin-eind herhaling onzekerheid 1:26
  - begin-eind isomorf onzekerheid 25:26
  - herhaalde letters scheppen meer zekerheid

Voorbeeld

- polyalbetische substitutie
  klaaralfabet standaard, cijferalfabet gemengd
- twee isologe cryptogrammen, andere sleutel
  respectievelijk periode = 3 en periode = 4
- opgave: reconstrueer cijferalfabet

```
K-1: 123123123123123123123123123123123123123...
C-1: QWYXTEXBUPRNTRKDJZVLFILUELRXTEXBUPRN...
K-2: 123412341234123412341234123412341234...
C-2: BQTRZDWSGIPACVGPPSIRZDWSPSIRZDWSGIPA...
```

Er onstaan 12 groepen isomorfe relaties
BQ,CT,PE en QW,VR,SL en TY,GK,IR enz.

Cijferalfabet verschoven

sleutel-1: G → Q **sleutel-2: G → B** **BQ**

sleutel-1: U → E **sleutel-2: U → P** **PE**

sleutel-1: X → T **sleutel-2: X → C** **CT**

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
F	B	S	V	U	X	Q	M	H	D	L	R	I	Z	W	P	K	G	C	A	E	N	Y	T	O	J
N	Y	T	O	J	F	B	S	V	U	X	Q	M	H	D	L	R	I	Z	W	P	K	G	C	A	E
	B	-	-	-	-	Q												C1					C2		
	B1					B2												C	-	-	-	-	T		
															P	-	-	-	-	E					

Afstanden in cijferalfabet voor BQ - CT - PE - etc.

Alle isomorfe relaties

A1-B1	QB	TC	EP	TC	ZH	QB
A2-B2	WQ	RV	LS	RV	HF	CL
A3-B3	YT	KG	RI	KG	BS	XQ
A1-B4	XR	DP	XR	DP	YS	QI
A2-B1	TZ	JP	TZ	HO	SC	ZV
A3-B2	ED	ZS	ED	BK	NL	GQ
A1-B3	XW	VI	XW	YX	HG	CB
A2-B4	BS	LR	BS	SV	TO	WP
A3-B1	UG	FZ	UG	NH	IJ	WB
A1-B2	PI	ID	PI	HX	ZL	XS
A2-B3	RP	LW	RP	TB	BX	IK
A3-B4	NA	US	NA	IL	TN	

A3-B3 identiek A2-B4 ➔ combineren

Reconstructie

A3-B3	YT	KG	RI	KG	BS	XQ
A2-B4	BS	LR	BS	SV	TO	WP

Isomorfie betekent voor afstanden in cijferalfabet:
als Y naast T dan ook K naast G en R naast I …

Maar ook mogelijk
Y-T en K-G en R-I …
Y--T en K--G en R--I …
Y---T en K---G en R---I …
…

Wat nu?

Stap 1 in het oplossen: kies maar

Rijg kettingen

A3-B3&A2-B4	YT	KG	RI	BS	XQ	LR	SV	TO	WP

YT + TO → YTO LR + RI → LRI BS + SV → BSV

Eerste benadering cijferalfabet

BSV --?-- LRI --?-- YTO --?-- KG --?-- WP --?-- XQ

Tweede dimensie

A3-B3&A2-B4	YT	KG	RI	BS	XQ	LR	SV	TO	WP
A2-B3	RP	LW	RP	TB	BX	IK			

alle isomorfe relaties in principe anders
bijvoorbeeld YT en R---P i.p.v. RP
dus RP niet zomaar in te voegen

remedie: niet horizontaal maar verticaal plaatsen van A2-B3

	T												I				L	R			B				
	B	S	V		L	R	I		Y	T	O		K	G			W	P			X	Q			
					W																				

Combineren

	T												I				L	R			B				
	B	S	V		L	R	I		Y	T	O		K	G			W	P			X	Q			
					W																				

	T																								
	B	S	V		L	R	I		Y	T	O														
	X	Q			W	P	K	G																	

	Y	T	O																						
		B	S	V							L	R	I												
		X	Q								W	P	K	G											

Zoek derde relatie

A1-B1	QB	TC	EP	TC	ZH	QB
A2-B2	WQ	RV	LS	RV	HF	CL
A3-B3	YT	KG	RI	KG	BS	XQ
A1-B4	XR	DP	XR	DP	YS	QI
A2-B1	TZ	JP	TZ	HO	SC	ZV
A3-B2	ED	ZS	ED	BK	NL	GQ
A1-B3	XW	VI	XW	YX	HG	CB
A2-B4	BS	LR	BS	SV	TO	WP
A3-B1	UG	FZ	UG	NH	IJ	WB
A1-B2	PI	ID	PI	HX	ZL	XS
A2-B3	RP	LW	RP	TB	BX	IK
A3-B4	NA	US	NA	IL	TN	

Y	T	O	
	B	S	V
	X	Q	

	L	R	I	
	W	P	K	G

X				
D	L	R	I	
	W	P	K	G

Meer relaties toevoegen

	Y	T	O							X	Q													
		B	S	V						D	L	R	I											
		X	Q								W	P	K	G										

A1-B2	PI	ID	PI	HX	ZL	XS

	Y	T	O							X	Q			D										
		B	S	V					H	D	L	R	I											
		X	Q							Z	W	P	K	G										

Concentreer op één lijn

	Y	T	O												X	Q			D					
		B	S	V							X	Q		H	D	L	R	I						
		X	Q												Z	W	P	K	G					

										Y	T	O												
											B	S	V		X	Q			D					
											X	Q		H	D	L	R	I						
															Z	W	P	K	G					

										Y	T	O												
						Y	T	O			B	S	V		X	Q			D					
		Y	T	O			B	S	V		X	Q		H	D	L	R	I						
			B	S	V		X	Q							Z	W	P	K	G					

Completeer

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

Geheel gereconstrueerd cijferalfabet

Oorspronkelijk alfabet?

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

Is het nu EN of E-N of E--N of … ?

het antwoord is soms niet nodig

wel nodig? bepaal de juiste decimatie van het alfabet

Decimatie

1	F	B	S	V	U	X	Q	M	H	D	L	R	I	Z	W	P	K	G	C	A	E	N	Y	T	O	J
3	F	V	Q	D	I	P	C	N	O	B	U	M	L	Z	K	A	Y	J	S	X	H	R	W	G	E	T
5	F	X	L	P	E	J	U	D	W	A	O	V	H	Z	C	T	S	M	I	G	Y	B	Q	R	K	N
7	F	M	W	N	S	D	K	T	U	R	C	J	Q	Z	E	B	H	P	Y	V	L	G	O	X	I	A
9	F	D	C	B	L	A	S	R	E	V	I	N	U	Z	Y	X	W	T	Q	P	O	M	K	J	H	G
11	F	R	Y	M	C	V	W	J	L	N	Q	G	S	Z	O	D	E	X	K	B	I	T	H	A	U	P
15	F	P	U	A	H	T	I	B	K	X	E	D	O	Z	S	G	Q	N	L	J	W	V	C	M	Y	R
17	F	G	H	J	K	M	O	P	Q	T	W	X	Y	Z	U	N	I	V	E	R	S	A	L	B	C	D
19	F	A	I	X	O	G	L	V	Y	P	H	B	E	Z	Q	J	C	R	U	T	K	D	S	N	W	M
21	F	N	K	R	Q	B	Y	G	I	M	S	T	C	Z	H	V	O	A	W	D	U	J	E	P	L	X
23	F	T	E	G	W	R	H	S	X	J	Y	A	K	Z	L	M	U	B	O	N	C	P	I	D	Q	V
25	F	J	O	T	Y	N	E	A	C	G	K	P	W	Z	I	R	L	D	H	M	Q	X	U	V	S	B

Lange isomorfen

NDEGMBYMLUKGLIZLKVXDZZXJQBOOUOM
HAVBINRIPWTBPLQPTKUAQQUZXNYYWYI

NDEGMBYMLUKGLIZLKVXDZZXJQBOOUOM
HAVBINRIPWTBPLQPTKUAQQUZXNYYWYI

JZQXUW MILP GBNH EVKT OYR DA

Zie ook het voorbeeld in de syllabus!