Cursus Cryptografie

TRANSPOSITIE

05-02-2017

Klassieke systemen

Transpositie
- Route
- Kolom
- Rooster

Monoalfabetisch
- Caesar
- Homofoon
- Monome-dinome
- Playfair
- Bifid

Gemengd
- ADFGVX
- Nomenclatuur
- Code
- Encicode

Polyalfabetisch
- Porta
- Vigenère
- Beaufort
- Nihilist
- Progressie

- Autoclaaf
- Wheatstone
- Multiplex
- One-time-pad

Machine
- Hagelin
- Kryha
- Enigma
- Purple

Transpositie

Kenmerken:
- permutatie elementen klaartekst
- transpositieblok vorm en afmetingen
- uitvullen transpositieblok
- volgorde inschrijven en uitnemen

Behandeld op college:
- route
- kolom uitgevuld
- kolom niet-uitgevuld
- kolom met gaten
- US Army double transposition
- turning grille

Civil War

Bericht van president Lincoln aan generaal majoor Burnside, gedateerd Washington, November 25, 1862

BURNSIDE, Falmouth, Virginia

Can Inn Ale me withe 2 oar our
Annpas Ann me flesh ends N.V.
Corn Inn out with U and Inn
Heaven day nest Wed roe Moore
Tom darkey hat greek a Why
Hawk of Abbott Inn B chewed I if.

BURNSIDE, Falmouth, Virginia

If I should be in a boat off Aguia Creek at dark tomorrow, Wednesday evening, could you, without inconvenience, meet me and pass an our of two with me?
A. Lincoln

Lincoln – 1 juni 1863

KLAARTEKST For Colonel Ludlow. Richardson and Brown, correspondents of the Tribune, captured at Vicksburg, are detained at Richmond. Please ascertain why they are detained and get them off if you can. The President U.S.

CRYPTOGRAM guard adam them they at wayland brown for kissing venus correspondents at neptune are off nelly turning up can get why detained tribune and times richardson the are ascertain and you fills belly this if detained please odor of ludlow commissioner

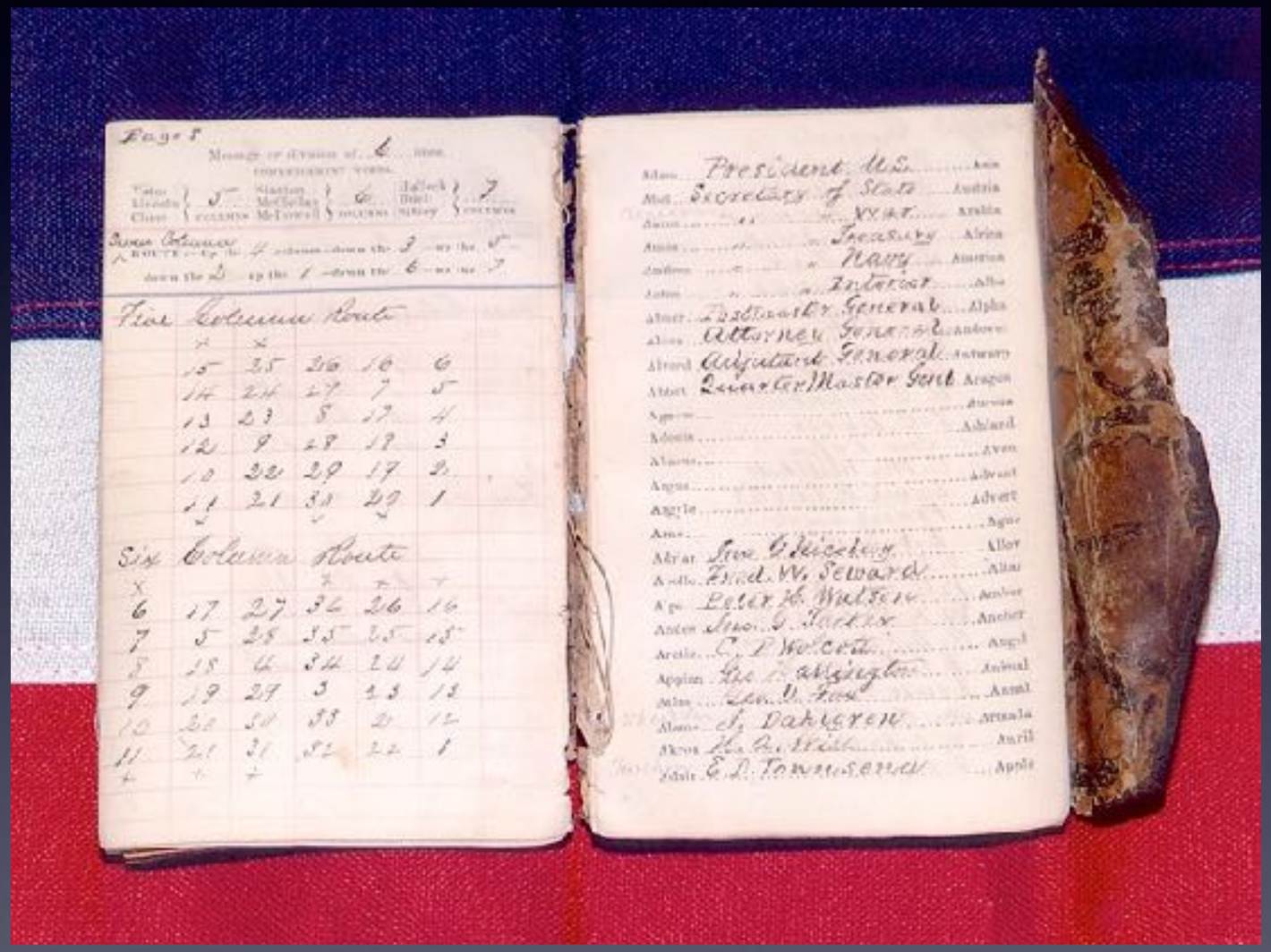
Union codeboek

indicator GUARD
5x7 route tramp

null zonder betekenis

vulling op lege plaats

codewoorden
adam = President US
nelly = 4:30 pm
neptune = Richmond
odor = Vicksburg
wayland = captured
venus = colonel



Indicator GUARD

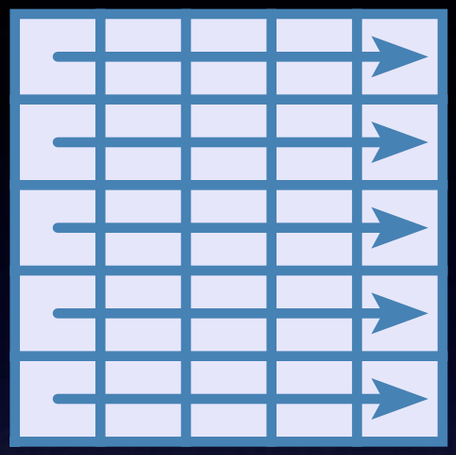
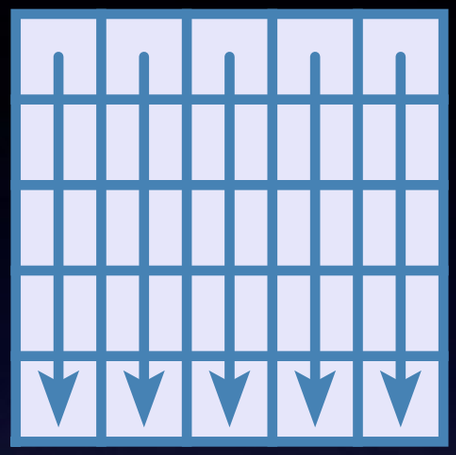
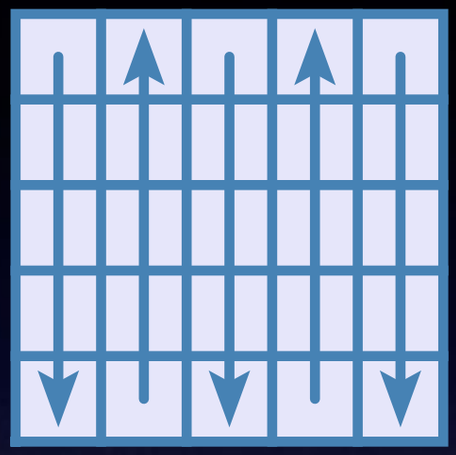
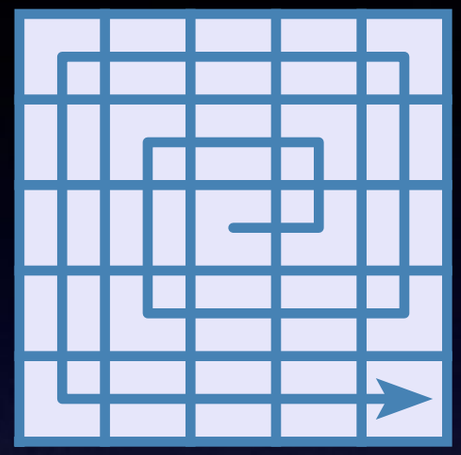
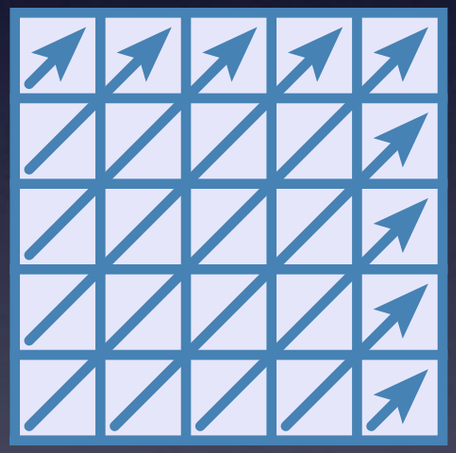
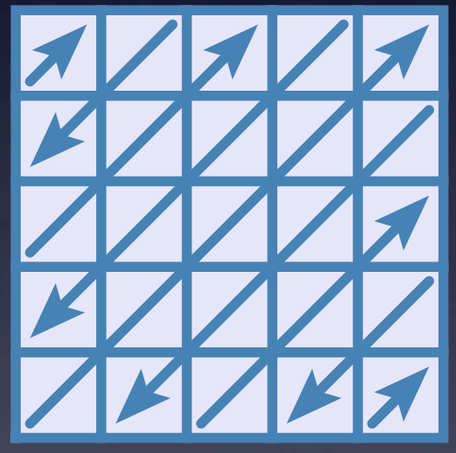
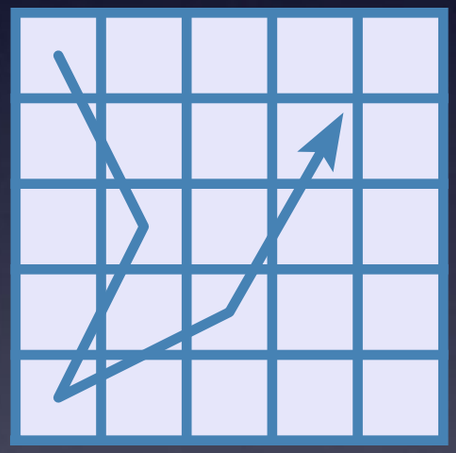
→	↓	STOP	↓	←
kissing	↓	commissioner	↓	times
for	venus	Ludlow	Richardson	and
Brown	correspondents	of	the	Tribune
wayland	at	odor	are	detained

at	neptune	please	ascertain	why
they	are	detained	and	get
them	off	if	you	can
adam	nelly	this	fills	up
↑	turning	↑	belly	↑
↑	↓	↑	←	↑
↑ START ↑	→	→	→	↑

Route transpositie

klaartekst: MAKKERS STAAKT UW WILD GERAAS
cryptogram: MRAWE ASKIR KSTLA KTUDA EAWGS

Route transpositie

3	16	9	22	15
20	8	21	14	2
7	25	13	1	19
24	12	5	18	6
11	4	17	10	23

- exotische routes zijn paardsprong, magisch vierkant
- verschillende route voor inschrijven en uitnemen
- spiraal routes leveren leesbare brokstukken

Kolomtranspositie

M	*U*	*S*	*K*	*U*	*S*
2	*5*	*3*	*1*	*6*	*4*
D	E	V	R	A	G
E	N	V	A	N	H
E	T	T	E	N	T
A	M	E	N	Z	Y
N	N	O	G	G	E
H	E	I	M	X	X

←transpositieblok uitgevuld

```
pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM XX
ct: RAENG MDEEA NHVVT EOIGH TYEXE NTMNE ANNZG X
```

kolomsplitsing is eenduidig

```
RAENGM DEEANH VVTEOI GHTYEX ENTMNE ANNZGX
```

Transpositie sleutel

M	U	S	K	U	S
M	U	S	1	U	S
2	U	S	1	U	S
2	U	3	1	U	S
2	U	3	1	U	4
2	5	3	1	U	4
2	5	3	1	6	4
2	5	3	1	6	4

Vervang de letters één voor één door cijfers in de volgorde van het alfabet

MUSKUS → 253164

Kolomtranspositie

M	*U*	*S*	*K*	*U*	*S*
2	*5*	*3*	*1*	*6*	*4*
D	E	V	R	A	G
E	N	V	A	N	H
E	T	T	E	N	T
A	M	E	N	Z	Y
N	N	O	G	G	E
H	E	I	M		

←transpositieblok niet uitgevuld

pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM XX
ct: RAENG MDEEA NHVVT EOIGH TYEEN TMNEA NNZG

kolomsplitsing niet eenduidig

RAENGM DEEANH VVTEOI GHTYEE NTMNE ANNZG
RAENGM DEEANH VVTEOI GHTYE ENTMNE ANNZG
RAENG MDEEA NHVVTE OIGHTY EENTMN EANNZG

Onregelmatige kolommen

2	1	4	7	3	6	5
	A	A		N		V
A				L		
O		P	P	E		A
R	L	H	A	R		B
O	U	R	D	O	O	R
J	A	P	A	N		

```
pt: AANVAL OP PEARL HARBOUR DOOR JAPAN
ct: ALUAA OROJN LERON APHRP VABRO PADA
```

Onregelmatig blok maakt opsplitsing nog moeilijker
- Japanse K10 rond 1940 oververcijfering J19 code
- Zendia transposities

Dubbele transpositie

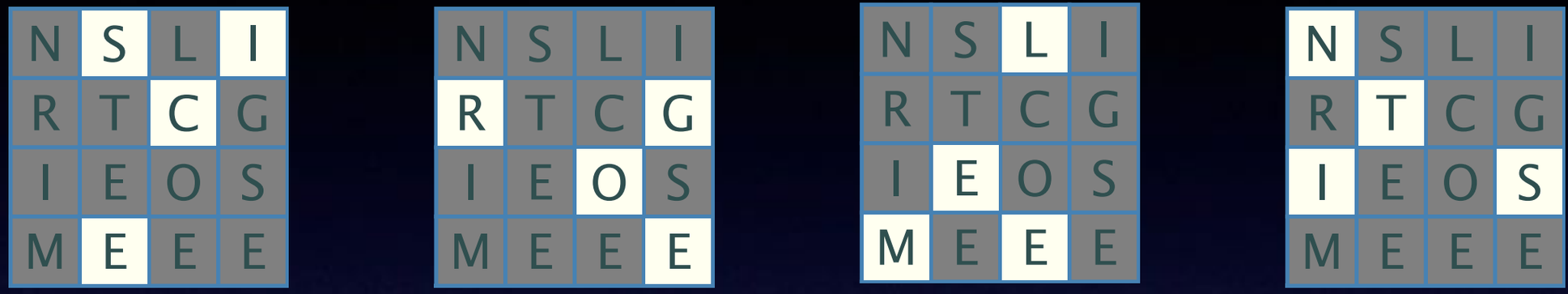
H	*A*	*R*	*I*	*N*	*G*	*T*	*O*	*N*
3	*1*	*8*	*4*	*5*	*2*	*9*	*7*	*6*
D	E	N	B	R	I	E	L	V
O	O	R	D	E	G	E	U	Z
E	N	G	E	V	A	L	L	E
N	A	L	V	A	N	A	A	R
M	A	D	R	I	D			

L	*E*	*E*	*S*	*B*	*R*	*I*	*L*
5	*2*	*3*	*8*	*1*	*7*	*4*	*6*
E	O	N	A	A	I	G	A
N	D	D	O	E	N	M	B
D	E	V	R	R	E	V	A
I	V	Z	E	R	L	U	L
A	N	R	G	L	D	E	E
L	A						

pt: DEN BRIEL VOOR DE GEUZEN GEVALLEN ALVA NAAR MADRID
ct: AERRL ODEVN ANDVZ RGMVU EENDI ALABA LEINE LDAOR EG

US Army Double Transposition

Turning grille




```
pt: SIC ERGO ELEMENTIS
ct: NSLIR TCGIE OSMEE E
```

Ook genoemd: Fleissner rooster
Oudste: Stadhouder Willem IV in 1745
Laatste: Duitse leger in 1917