

# Classical Cryptography

## Basics: transpositions

Karst Koymans

Informatics Institute

University of Amsterdam

(version 22.6, 2023/02/16 13:53:54 UTC)

Friday, February 17, 2023

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples

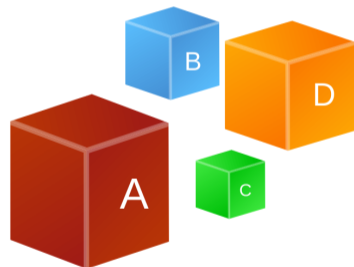
# Substitutions versus Transpositions

- Substitutions
  - transform objects into or replace objects by other objects
  - keeping the positions of these objects the same
- Transpositions
  - put the objects into a different position
  - keeping the identity of these objects the same
- Both operations can be represented by permutations
  - with paying careful attention to the semantics of each permutation **and its inverse**

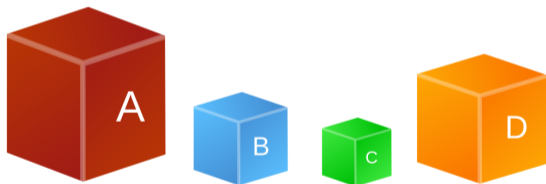
# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples

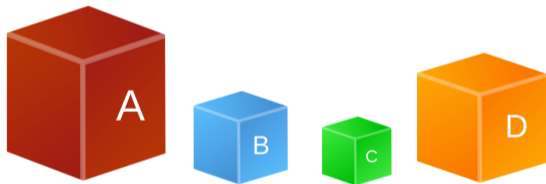
# Is this a permutation?



# And now?



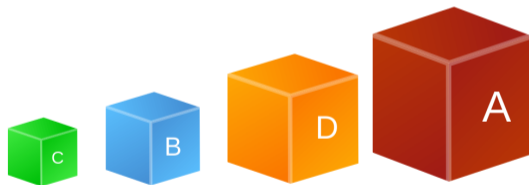
# And now?



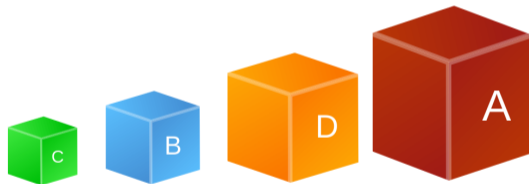
Do we order by identity, alphabetically?  $A < B < C < D$ ?



# Or maybe like this?



Or maybe like this?



Do we order by size? tiny<small<big<huge (C<B<D<A)?

# And more options...



# And more options...

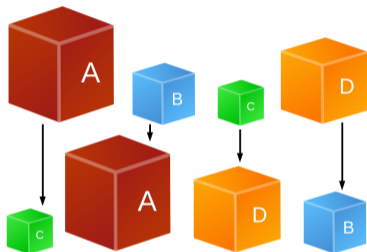


Ordered by color: red < orange < green < blue (A < D < C < B)

# Case studies...

- In all of the following examples we have that
  - The position of A in the top row is the same as the position of C in the bottom row
  - The position of B in the top row is the same as the position of A in the bottom row
  - The position of C in the top row is the same as the position of D in the bottom row
  - The position of D in the top row is the same as the position of B in the bottom row
- So in some sense we always have  $A \rightarrow C \rightarrow D \rightarrow B \rightarrow A$
- With the standard notation 
$$\begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$$

# Keeping position, but changing identity (1)

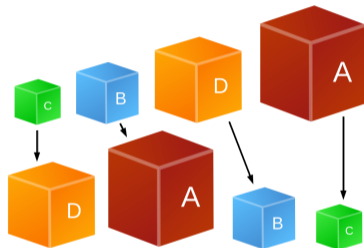


$$1 \quad 2 \quad 3 \quad 4 \quad \left( \begin{array}{cccc} A & B & C & D \\ C & A & D & B \end{array} \right)$$

$$\boxed{\begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}}$$

$$\boxed{1 \quad 2 \quad 3 \quad 4}$$

# Keeping position, but changing identity (2)

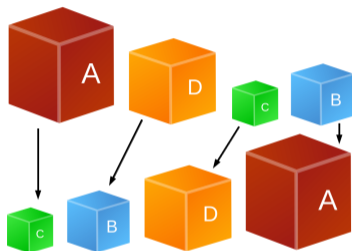


$$\begin{array}{cccc}
 1 & 2 & 3 & 4 \\
 \left( \begin{array}{cccc}
 A & B & C & D \\
 C & A & D & B
 \end{array} \right)
 \end{array}$$

$$\left( \begin{array}{cccc}
 C & B & D & A \\
 D & A & B & C
 \end{array} \right)$$

$$\boxed{4 \ 2 \ 1 \ 3}$$

# Keeping position, but changing identity (3)



$$\begin{array}{cccc}
 1 & 2 & 3 & 4 \\
 \left( \begin{array}{cccc}
 A & B & C & D \\
 C & A & D & B
 \end{array} \right)
 \end{array}$$

$$\left( \begin{array}{cccc}
 A & D & C & B \\
 C & B & D & A
 \end{array} \right)$$

$$\left( \begin{array}{cccc}
 1 & 4 & 3 & 2
 \end{array} \right)$$



## Case studies for positions...

- We still have that
  - The position of A in the top row is the same as the position of C in the bottom row
  - The position of B in the top row is the same as the position of A in the bottom row
  - The position of C in the top row is the same as the position of D in the bottom row
  - The position of D in the top row is the same as the position of B in the bottom row
- What changes is that we look at the effect on the positions
- Also notice the direction of the arrows from bottom to top
  - which as we will see is more natural

# Legacy and modern notation for positions

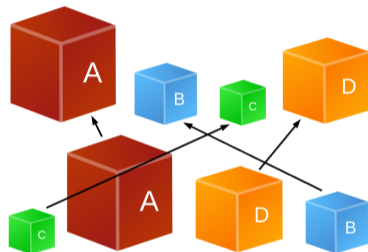
- It would be consistent to also use modern notation for positions and their permutations, like this

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix}$$

- But in order not to create more confusion at this stage, I will use the more standard notation like

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

# Keeping identity, but changing position (1)

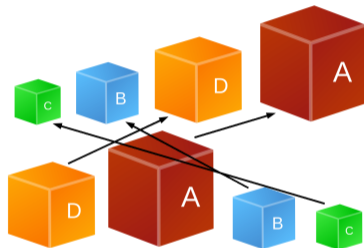


$$\begin{array}{cccc}
 A & B & C & D \\
 \left( \begin{array}{cccc}
 1 & 2 & 3 & 4 \\
 3 & 1 & 4 & 2
 \end{array} \right)
 \end{array}$$

$$\left( \begin{array}{cccc}
 2 & 4 & 1 & 3 \\
 1 & 2 & 3 & 4
 \end{array} \right)$$

$$\boxed{C \ A \ D \ B}$$

# Keeping identity, but changing position (2)

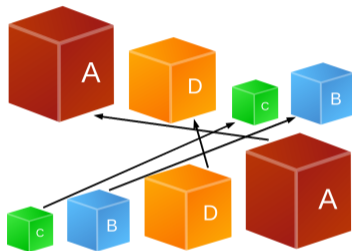


$$\begin{array}{cccc}
 A & B & C & D \\
 \left( \begin{array}{cccc}
 1 & 2 & 3 & 4 \\
 3 & 4 & 2 & 1
 \end{array} \right)
 \end{array}$$

$$\left( \begin{array}{cccc}
 2 & 3 & 4 & 1 \\
 4 & 2 & 1 & 3
 \end{array} \right)$$

$$\boxed{D \ A \ B \ C}$$

# Keeping identity, but changing position (3)



$$\begin{array}{cccc}
 A & B & C & D \\
 \left( \begin{array}{cccc}
 1 & 2 & 3 & 4 \\
 3 & 4 & 2 & 1
 \end{array} \right)
 \end{array}$$

$$\left( \begin{array}{cccc}
 4 & 2 & 1 & 3 \\
 1 & 4 & 3 & 2
 \end{array} \right)$$

$$\boxed{C \ B \ D \ A}$$

# Commuting diagram (before: $f$ ; after: $g$ )

$$\begin{array}{ccc} P & \xrightarrow{f} & O \\ \tau \uparrow & & \downarrow \sigma \\ P & \xrightarrow{g} & O \end{array}$$

- $P$  is the set of positions
- $O$  is the set of objects (or identities)
- $\sigma$  is a substitution (of identity) permutation
- $\tau$  is a transposition (change of position) permutation

# Permutation directions

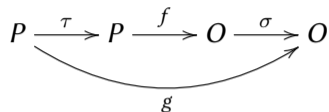
- Consider the transformation from top ( $f$ ) to bottom ( $g$ )
- $g = \sigma \circ f \circ \tau$
- $g^{-1} = \tau^{-1} \circ f^{-1} \circ \sigma^{-1}$
- Notice the direction of the permutations and their inverses
  - The substitution permutation from top ( $f$ ) to bottom ( $g$ )
  - The transposition permutation from bottom ( $g$ ) to top ( $f$ )
- When reversing top and bottom things turn around
  - $f = \sigma^{-1} \circ g \circ \tau^{-1}$
  - $f^{-1} = \tau \circ g^{-1} \circ \sigma$

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples



## Texts as strings or sequences of characters



- $P$  is  $n$ , where  $n = \{0, \dots, n - 1\}$
- $O$  is  $\{A, B, C, \dots, X, Y, Z\}$ , our alphabet
- $f$  is the plaintext<sup>1</sup> before encryption
  - or the ciphertext before decryption
- $g = \sigma \circ f \circ \tau$  is the ciphertext after encryption
  - or the plaintext after decryption

---

<sup>1</sup>Note that in this case  $f$  doesn't need to be injective nor surjective

# Relation between transposition and substitution

- Even though transposition and substitution seem unrelated they are kind of dual to each other
- Both are permutations (of position, respectively identity)
- Transposition contributes to Shannon's "diffusion"
- Substitution contributes to Shannon's "confusion"
- Taken together we might<sup>2</sup> call them
  - **su(b)positions**
  - **trans(s)titutions**

---

<sup>2</sup>This is in no way standard or accepted terminology

# Relaxing bijectivity of substitutions and transpositions

$$\begin{array}{ccccc}
 P' & \xleftarrow{\tau'} & P & \xrightarrow{f} & O & \xleftarrow{\sigma'} & O' \\
 & \xrightarrow{\tau} & & & & \xrightarrow{\sigma} & 
 \end{array}$$

- In the case that  $f$  is the given plaintext
  - $\sigma$  only needs to be injective, but not surjective
    - $id_O = \sigma' \circ \sigma$
    - $O'$  can be “bigger” than  $O$
  - $\tau$  only needs to be surjective, but not injective
    - $id_P = \tau \circ \tau'$
    - $P'$  can be “bigger” than  $P$

# Expansion and compression

- Suppose that  $P'$  is indeed “bigger” than  $P$
- We might use the following terminology if  $id_P = \tau \circ \tau'$ 
  - $\tau$  is used for **expansion**
  - $\tau'$  is a corresponding **compression**
    - Mathematically speaking  $\tau'$  is a **section** of  $\tau$

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions**
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples

# Transposition that doesn't hide much

## Internet meme (Cambridge research ???)

Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttar in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

(" (sic)" deleted; "e" changed into "a"; comma inserted)

Source: <https://www.mrc-cbu.cam.ac.uk/people/matt.davis/cmabridge/>

# Transposition that doesn't hide much

## Internet meme (Cambridge research ???)

According to a researcher at Cambridge University, it doesn't matter in what order the letters in a word are, the only important thing is that the first and last letter be at the right place. The rest can be a total mess and you can still read it without problem. This is because the human mind does not read every letter by itself, but the word as a whole.

(" (sic)" deleted; "e" changed into "a"; comma inserted)

Source: <https://www.mrc-cbu.cam.ac.uk/people/matt.davis/cmabridge/>

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions**
  - Geometric/Route ciphers**
  - Permutation ciphers
  - Historic examples



# Generating transpositions (1): Skytale



CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=1698345>

# The Skytale (Scytale)

- Already used by the Spartan general Lysander
- Narrow parchment wound around a piece of wood of a given diameter
- Each side of the communication channel needs an identical piece of wood
- The length of wood is not important, as long as the message “fits”
- Encryption corresponds to a **simple columnar transposition**<sup>3</sup>
  - Decryption corresponds to a “row transposition”

---

<sup>3</sup>Some call this an example of a route transposition

# Simple columnar (route) transposition

$$\begin{pmatrix} 0 & 1 & \dots & c-1 \\ c & c+1 & \dots & 2c-1 \\ \dots & \dots & \dots & \dots \\ (r-1)c & (r-1)c+1 & \dots & rc-1 \end{pmatrix}$$

- $r$  corresponds to the circumference (measured in letters) of the wooden stick
- The total length of the message is  $rc$
- The plaintext is written in row by row
- The ciphertext is read out column by column

# Formulas relating a text string to the rectangular block

- From rectangle to string row by row

$$(i, j) \mapsto ic + j$$

- From string to rectangle row by row

$$i \mapsto ([i/c], i \pmod{c})$$

- From rectangle to string column by column

$$(i, j) \mapsto jr + i$$

- From string to rectangle column by column

$$i \mapsto (i \pmod{r}, [i/r])$$

## Generating transpositions (2): Railfence

- A railfence cipher has as key information only the depth of the fence
  - and maybe a starting direction (down or up)
- Items are written in a zigzag pattern going down and up (or up and down) the fence
- It can be described as an inefficient row transposition with holes (grille)
- Also, by zigzagging left and right (or right and left),  
it can be described as a columnar transposition with holes

## Generating transpositions (3): Routes

There are many more ways to traverse a rectangle  
or for that matter any other geometric shape

### Exercise

Match Colonel Parker Hitt's methods from Figure 3.2 in Holden's book with the route ciphers from Figure 2.2 in Hans van der Meer's syllabus

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions**
  - Geometric/Route ciphers
  - Permutation ciphers**
  - Historic examples

# Permutation(s of positions) ciphers

- Divide the plaintext into blocks of  $n$  letters and apply (the same) position permutation to each block separately
- The last block is padded with “nulls”
  - The permutation maps a ciphertext position to a plaintext position

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \begin{array}{l} \text{cipher position} \\ \text{plain position} \end{array}$$

- This permutation is the same as given by the following mapping

$$\begin{pmatrix} 4 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \begin{array}{l} \text{cipher position} \\ \text{plain position} \end{array} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \quad \begin{array}{l} \text{plain position} \\ \text{cipher position} \end{array}$$

- **Warning: confusion! A permutation or its inverse?**  
In The Mathematics of Secrets this is also denoted by the string “4132”
- A string can be remembered by using a keyword, like “TALE” for the sequence 4132, using the alphabetic order



# Permutation cipher compositions (products)

- Suppose the block sizes are  $p$  and  $q$
- Then the block size of the product is given by
  - $\text{lcm}(p, q)$ , the least common multiple of  $p$  and  $q$
- Hence in the case of  $p = q$  you get nothing new

# Keyed columnar transpositions

- These are compositions (products) of permutations and routes
  - First the permutation and then the “row-in-column-out” route
  - What happens if you do it the other way around?
- They offer a better diffusion of the plaintext throughout the whole ciphertext
- There is still no confusion though
- Shannon argued that both confusion and diffusion are important
  - We will see later how modern block ciphers achieve both

# Outline

- 1 Theoretic considerations
  - Permutations
- 2 Framework for cryptography
- 3 Transpositions**
  - Geometric/Route ciphers
  - Permutation ciphers
  - Historic examples**

# A historic transposition

## Battle of Fredericksburg

Washington, D.C., November 25, 1862

To general Burnside, Falmouth, Virginia

Can Inn Ale me withe 2 oar our Ann pas Ann me flesh ends N. V. Corn Inn out with U cud Inn  
heaven day nest We roe Moore Tom darkey hat Greek Why Hawk of Abbott Inn B chewed I if.

From whom?

# Transpositions

Adapted from slides by Hans van der Meer

# Civil War

Message of president Lincoln to general major Burnside,  
dated Washington, November 25, 1862

BURNSIDE, Falmouth, Virginia  
Can I see you with the 2nd of our  
Army as you are in the N. V.  
Army out with you and I  
will be with you on the 25th  
of the month. I will be with  
you on the 25th of the month.  
I will be with you on the 25th  
of the month. I will be with  
you on the 25th of the month.

BURNSIDE, Falmouth, Virginia  
If I should be in a boat off Aquia  
Creek at dark tomorrow,  
Wednesday evening, could you,  
without inconvenience, meet me  
and pass an hour or two with  
me? A. Lincoln

# Lincoln – June 1, 1863

**PLAINTEXT** 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





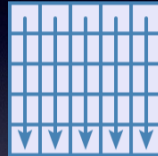
# Indicator GUARD

→	↓	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 transposition

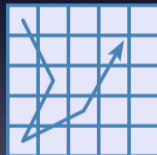
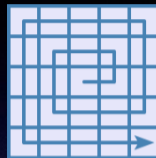
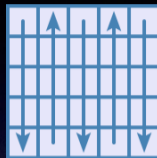
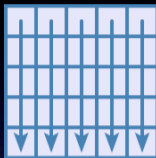
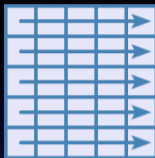


M	A	K	K	E
R	S	S	T	A
A	K	T	U	W
W	I	L	D	G
E	R	A	A	S



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

# Route transposition



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

- exotic routes are knight tour, magic square
- different routes for write-in and read-out
- spiral routes show readable fragments

# Column transposition

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

← transposition block filled completely

pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM XX

ct: RAENG MDEEA NHVVT EOIGH TYEXE NTMNE ANNZG X

Column division is unambiguous

RAENGM DEEANH VVTEOI GHTYEX ENTMNE ANNZGX

# Transposition key

	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

Replace the letters of the key, one by one, by digits in alphabetic order

MUSKUS → 253164

# Column transposition

M	U	S	K	U	S
2	5	3	7	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		

← transposition block **not**  
completely filled

pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM

ct: RAENG MDEEA NHVVT EOIGH TYEEN TMNEA NNZG

## Column division ambiguous

RAENGM DEEANH VVTEOI GHTYEE NTMNE ANNZG

RAENGM DEEANH VVTEOI GHTYE ENTMNE ANNZG

RAENG MDEEA NHVVTE OIGHTY EENTMN EANNZG

# Column transposition

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

Irregular block makes division even harder

- Japanese K1 around 1940 J19 encicode
- Zendia transpositions

# 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

N	S	L	I
R	T	C	G
I	E	O	S
M	E	E	E

0°

N	S	L	I
R	T	C	G
I	E	O	S
M	E	E	E

90°

N	S	L	I
R	T	C	G
I	E	O	S
M	E	E	E

180°

N	S	L	I
R	T	C	G
I	E	O	S
M	E	E	E

270°

pt: SIC ERGO ELEMENTIS  
ct: NSLIR TCGIE OSMEE E

Also called a “Fleissner grille”  
Oldest: Stadtholder Willem IV in 1745  
Latest: German army in 1917