Cryptography (and Information Security) 6CCS3CIS / 7CCSMCIS

Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 3.4: Transposition ciphers

Table of contents I

1. Transposition ciphers
   - Rail fence cipher
   - Rotating (turning) grilles
   - Multiple-stage columnar transposition cipher

Transposition ciphers

Transposition cipher

Perform some sort of permutation on the plaintext letters.
Works on blocks of letters of the plaintext.

More formally:

- For block length t, let $\mathcal{K}$ be the set of permutations on $\{1, \ldots, t\}$. For each $e \in \mathcal{K}$ and $m \in \mathcal{M}$

$$E_e(m) = m_{e(1)} m_{e(2)} \cdots m_{e(t)}$$

- The set of all such transformations is called a transposition cipher.
- To decrypt $c = c_1 c_2 \cdots c_t$ compute $D_d(c) = c_{d(1)} c_{d(2)} \cdots c_{d(t)}$, where d is inverse permutation.
- Letters unchanged so one can exploit frequency analysis for dipthongs, tripthongs, words, etc.

Let us see three examples.

Table of contents I

1 Transposition ciphers
- Rail fence cipher
- Rotating (turning) grilles
- Multiple-stage columnar transposition cipher

Rail fence cipher

Rail fence cipher (a.k.a. Zig-zag cipher)

Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. (Beware: variants exist under the same name.)

- For example, to encipher the message

  MEET ME AFTER THE TOGA PARTY

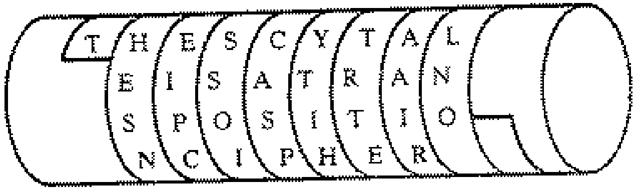
  with a rail fence of depth 2, we write:

  M E M A T R H T G P R Y
  E T E F E T E O A A T

  so that the ciphertext is

  MEMATRHTGPRYETEFETEOAAT

- Idea goes back to Greek scytale.



Scytale

Rail fence cipher

- As another example, to encipher the message

  WE ARE DISCOVERED FLEE AT ONCE

  with a rail fence of depth 3, we write:

```
W       E       C       R       L       T       E
  E   R   D   S   O   E   E   F   E   A   O   C
    A       I       V       D       E       N
```

  so that the ciphertext is

  WECRLTEERDSOEEFEAOCAIVDEN

- **Decryption**: reconstruct the diagonal grid used to encrypt the message.
  - Start by making a grid with as many rows as the key is, and as many columns as the length of the ciphertext.
  - Place the first letter in the top left square, and dashes diagonally downwards where the letters will be.
  - When we get back to the top row, we place the next letter in the ciphertext.
  - Continue like this across the row, and start the next row when you reach the end.

Rail fence cipher: decryption example

- If we receive the ciphertext “TEKOOHRACIRMNREATANFTETYTGHH” encrypted with a key of 4, we have a table with 4 rows because the key is 4, and 28 columns as the ciphertext has length 28.
- We start by placing the “T” in the first square, and then dash the diagonal down spaces until we get back to the top row, and place the “E” here. Continuing to fill the top row we get:

```
T           E           K           O           O
  -       -   -       -   -       -   -       -   -
    -   -       -   -       -   -       -   -       -
      -           -           -           -           -
```

- Continuing this row-by-row, we get the successive stages shown below:

```
T           E           K           O           O
  H       R   A       C   I       R   M       N   R
    -   -       -   -       -   -       -   -       -
      -           -           -           -           -
```

```
T           E           K           O           O
  H       R   A       C   I       R   M       N   R
    E   A       T   A       N   F       T   E       T
      -           -           -           -           -
```

Rail fence cipher: decryption example

- and finally

```
T           E           K           O           O
  H       R   A       C   I       R   M       N   R
    E   A       T   A       N   F       T   E       T
      Y           T           G           H           H
```

- From this we can now read the plaintext off following the diagonals to get:

THEY ARE ATTACKING FROM THE NORTH

Rail fence cipher

Rail fence cipher (a.k.a. Zig-zag cipher)

Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. (Beware: variants exist under the same name.)

- For example, to encipher the message

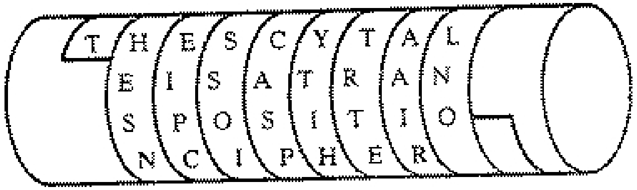
  MEET ME AFTER THE TOGA PARTY

  with a rail fence of depth 2, we write:

```
M   E   M   A   T   R   H   T   G   P   R   Y
  E   T   E   F   E   T   E   O   A   A   T
```

  so that the ciphertext is

  MEMATRHTGPRYETEFETEOAAT



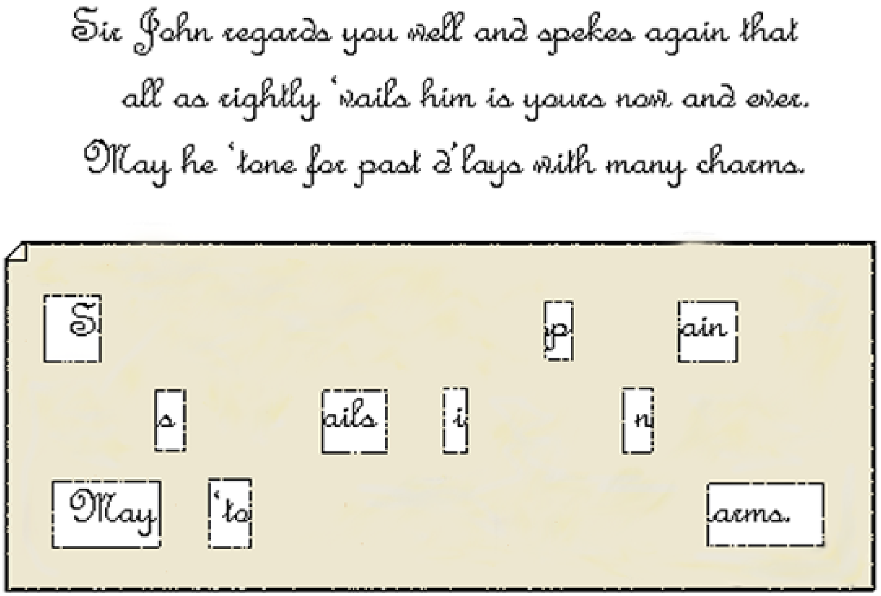
- Idea goes back to Greek scytale.
- Trivial to cryptanalyze.
  Hence, more clever transposition ciphers have been devised.

Table of contents I

1. Transposition ciphers
   - Rail fence cipher
   - Rotating (turning) grilles
   - Multiple-stage columnar transposition cipher

Cardano grille

- Girolamo Cardano (Italy, 16th cent., mathematician and Kabbalist).
- **Use a mask (“grille") with precut holes.**
    - Encoder writes plaintext in holes, removes mask, fills remainder with blind text, retaining appearance of an innocuous message.
    - Decryption: recipient must possess an identical mask (or must know spacing that created it).

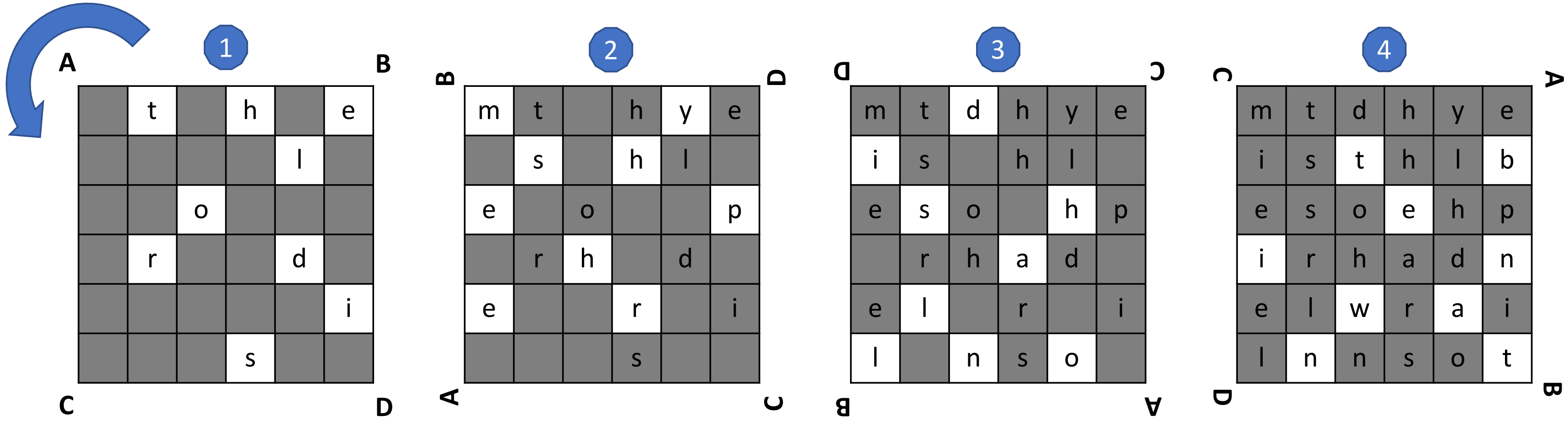


Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.

- Skipping letters within an otherwise plausible ciphertext.
- Is example of steganography, but provides basis for transposition.

Rotating (turning) grille (18th century)

- **Grille**: a sheet with a grid of squares, some of which are cut out.
- Example:
  - 6 × 6 grid of squares, of which 9 are cut out.
  - Plaintext: The Lord is my shepherd. I shall not be in want.
  - Write first 9 letters in each square cut out, left2right, top2bottom.
  - Turn grille by 90° in predetermined direction (e.g., counterclockwise).
  - Write next 9 letters... until grille is filled.
  - Read ciphertext (left2right, top2bottom): mtdhyeisthlbesoehpirhadnelwrailnnsot.



	t		h		e
				l	
		o			
	r			d	
					i
			s		

m	t		h	y	e
	s		h	l	
e		o			p
	r	h		d	
e			r		i
			s		

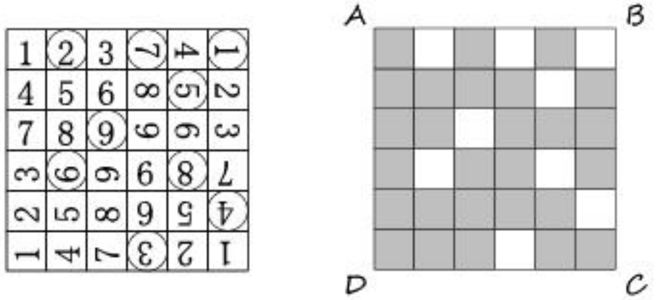
m	t	d	h	y	e
i	s		h	l	
e	s	o		h	p
	r	h	a	d	
e	l		r		i
l		n	s	o	

m	t	d	h	y	e
i	s	t	h	l	b
e	s	o	e	h	p
i	r	h	a	d	n
e	l	w	r	a	i
l	n	n	s	o	t

- Deciphering: write ciphertext in 6 × 6 grid and use rotating grid.

Rotating (turning) grille: preparation

- *When enciphering, every time the grille is turned, the cut out squares are precisely positioned at squares not yet filled.*
- Procedure to select squares of the grille to be cut out:
  - divide grid in 3×3 quadrants, number squares of each quadrant,
  - among four squares numbered “1”, select one to be cut out (e.g., rightmost square of top row) to ensure that each of these four squares is exposed exactly once during enciphering,
  - among four squares numbered “2”, one is selected to be cut out...



© S. Tomokiyo

Preparation of a rotating grille.

By choosing thus exactly one square to be cut out from among the four squares bearing the same number, it can be ensured that each square can be filled at one of the four rotating positions.

Other, more complex, grilles exist (but can all be attacked).

Table of contents I

1. Transposition ciphers
   - Rail fence cipher
   - Rotating (turning) grilles
   - Multiple-stage columnar transposition cipher

Columnar transposition cipher

- Write message in a rectangle, row by row, and read message off, column by column, but *permute the order of the columns*.
- The order of the columns thus is the key to the algorithm.
- For example, with key 4312567 (and with padding to fill the grid)

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z
Ciphertext:	TTNAAPTMTSUOAODWCOIXKNLYPETZ						

  To encrypt, start with column labeled 1, write down all letters in that column, proceed with column labeled 2, etc.
- A pure transposition cipher is easily recognized and attacked: ciphertext has same letter frequencies as original plaintext.

Multiple-stage columnar transposition cipher

- A transposition cipher (columnar or not) can be made significantly more secure by **performing more than one stage of transposition**.
- Result: more complex permutation that is not easily reconstructed.
- Let's reencrypt foregoing message

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

using the same algorithm:

Key:	4	3	1	2	5	6	7
Plaintext:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Ciphertext: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Multiple-stage columnar transposition cipher

- To visualize this double transposition, designate the 28 letters in original plaintext by their position:

01	02	03	04	05	06	07	08	09	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28

First transposition, still quite regular structure (+7 in blocks of 4!):

03	10	17	24	04	11	18	25	02	09	16	23	01	08
15	22	05	12	19	26	06	13	20	27	07	14	21	28

Second: less structured permutation (cryptanalysis more difficult):

17	09	05	27	24	16	12	07	10	02	22	20	03	25
15	13	04	23	19	14	11	01	26	21	18	08	06	28

Multiple stages of encryption can produce an algorithm that is significantly more difficult to cryptanalyze

This is as true of substitution ciphers as it is of transposition ciphers.

Before we see examples of this (rotor machines, DES, ...), let us say a few words about steganography.