Transposition cipher

In cryptography, a **transposition cipher** (also known as a permutation cipher) is a method of encryption which scrambles the positions of characters (*transposition*) without changing the characters themselves. Transposition ciphers reorder units of plaintext (typically characters or groups of characters) according to a regular system to produce a ciphertext which is a permutation of the plaintext. They differ from substitution ciphers, which do not change the position of units of plaintext but instead change the units themselves. Despite the difference between transposition and substitution operations, they are often combined, as in historical ciphers like the ADFGVX cipher or complex high-quality encryption methods like the modern Advanced Encryption Standard (AES).

Step-by-step process for the double columnar transposition cipher.

General principle

Plaintexts can be rearranged into a ciphertext using a key, scrambling the order of characters like the shuffled pieces of a jigsaw puzzle. The resulting message is hard to decipher without the key because there are many ways the characters can be arranged.

For example, the plaintext "THIS IS WIKIPEDIA" could be encrypted to "TWDIP SIHII IKASE". To decipher the encrypted message without the key, an attacker could try to guess possible words and phrases like DIATHESIS, DISSIPATE, WIDTH, etc., but it would take them some time to reconstruct the plaintext because there are many combinations of letters and words. By contrast, someone with the key could reconstruct the message easily:

```
C I P H E R     Key
1 4 5 3 2 6     Sequence (key letters in alphabetical order)
T H I S I S     Plaintext
W I K I P E
D I A * * *

Ciphertext by column:
  #1 TWD, #2 IP, #3 SI, #4 HII, #5 IKA, #6 SE
Ciphertext in groups of 5 for readability:
  TWDIP SIHII IKASE
```

In practice, a message this short and with a predictable keyword would be broken almost immediately with cryptanalysis techniques. Transposition ciphers have several vulnerabilities (see the section on "Detection and cryptanalysis" below), and small mistakes in the encipherment process can render the entire ciphertext meaningless.

However, given the right conditions - long messages (e.g., over 100–200 letters), unpredictable contents, unique keys per message, strong transposition methods, and so on - guessing the right words could be computationally impossible without further information. In their book on codebreaking historical ciphers, Elonka Dunin and Klaus Schmeh describe double columnar transposition (see below) as "one of the best manual ciphers known".[1]

Rail Fence cipher

The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows. For example, using three "rails" and a message of 'WE ARE DISCOVERED FLEE AT ONCE', the cipherer writes out:

```
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 . .
```

Then reads off:

```
WECRL TEERD SOEEF EAOCA IVDEN
```

(The cipher has broken this ciphertext up into blocks of five to help avoid errors. This is a common technique used to make the cipher more easily readable. The spacing is not related to spaces in the plaintext and so does not carry any information about the plaintext.)

Scytale

The rail fence cipher follows a pattern similar to that of the scytale, (pronounced "SKIT-uhl-ee") a mechanical system of producing a transposition cipher used by the ancient Greeks. The system consisted of a cylinder and a ribbon that was wrapped around the cylinder. The message to be encrypted was written on the coiled ribbon. The letters of the original message would be rearranged when the ribbon was uncoiled from the cylinder. However, the message was easily decrypted when the ribbon recoiled on a cylinder of the same diameter as the encrypting cylinder.[2] Using the same example as before, if the cylinder has a radius such that only three letters can fit around its circumference, the cipherer writes out:

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

In this example, the cylinder is running horizontally and the ribbon is wrapped around vertically. Hence, the cipherer then reads off:

```
WOEEV EAEAR RTEEO DDNIF CSLEC
```

Route cipher

In a route cipher, the plaintext is first written out in a grid of given dimensions, then read off in a pattern given in the key. For example, using the same plaintext that we used for rail fence:

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

The key might specify "spiral inwards, clockwise, starting from the top right". That would give a cipher text of:

```
EJXCTEDEC DAEWRIORF EONALEVSE
```

Route ciphers have many more keys than a rail fence. In fact, for messages of reasonable length, the number of possible keys is potentially too great to be enumerated even by modern machinery. However, not all keys are equally good. Badly chosen routes will leave excessive chunks of plaintext, or text simply reversed, and this will give cryptanalysts a clue as to the routes.

A variation of the route cipher was the Union Route Cipher, used by Union forces during the American Civil War. This worked much like an ordinary route cipher, but transposed whole words instead of individual letters. Because this would leave certain highly sensitive words exposed, such words would first be concealed by code. The cipher clerk may also add entire null words, which were often chosen to make the ciphertext humorous.

Columnar transposition

In the middle of the 17th century, Samuel Morland introduced an early form of columnar transposition. It was further developed much later, becoming very popular in the later 19th century and 20th century, with French military, Japanese diplomats and Soviet spies all using the principle.

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the keyword `ZEBRAS` is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword `ZEBRAS` and the message `WE ARE`

`DISCOVERED. FLEE AT ONCE`. In a regular columnar transposition, we write this into the grid as follows:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
```

providing five nulls (`QKJEU`), these letters can be randomly selected as they just fill out the incomplete columns and are not part of the message. The ciphertext is then read off as:

```
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
```

In the irregular case, the columns are not completed by nulls:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E
```

This results in the following ciphertext:

```
EVLNA CDTES EAROF ODEEC WIREE
```

To decipher it, the recipient has to work out the shape of the enciphering grid by dividing the message length by the key length to find the number of rows in the grid. The length of the grid's last line is given by the remainder. The key is written above the grid, and the ciphertext is written down the columns of the grid in the order given by the letters of the key. The plaintext appears on the rows. A partial decipherment of the above ciphertext, after writing in the first column:

```
6 3 2 4 1 5
. . . . E .
. . . . V .
. . . . L .
. . . . N .
.
```

In a variation, the message is blocked into segments that are the key length long and to each segment the same permutation (given by the key) is applied. This is equivalent to a columnar transposition where the read-out is by rows instead of columns.

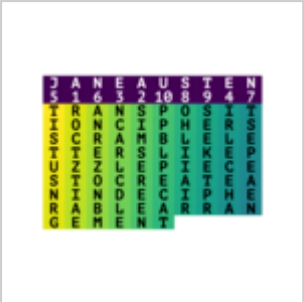
Columnar transposition continued to be used for serious purposes as a component of more complex ciphers at least into the 1950s.

Double transposition

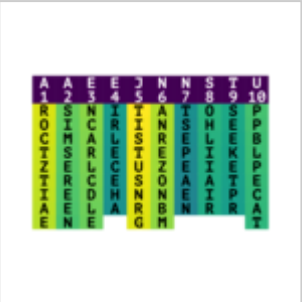
A single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.

Visual demonstration of double transposition

In the following example, we use the keys **JANEAUSTEN** and **AEROPLANES** to encrypt the following plaintext: "**Transposition ciphers scramble letters like puzzle pieces to create an indecipherable arrangement.**"

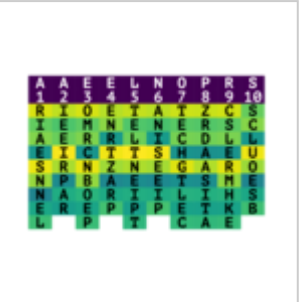


Step 1: The plaintext message is written into the first grid (which has the key JANEAUSTEN).



The columns are read off in alphabetical order according to the key, into the next grid (see step 2).

Step 2: The columns from step 1 are written into the second grid (which has the key AEROPLANES).



The columns are read off in alphabetical order according to the key, into the next grid (see step 3).

Step 3: The ciphertext is often written out in blocks of 5, e.g. **RIAES NNELI EEIRP** etc.

The colors show how the letters are scrambled in each transposition step. While a single step only causes a minor rearrangement, the second step leads to a significant scrambling effect if the last row of the grid is incomplete.

Another example

As an example, we can take the result of the irregular columnar transposition in the previous section, and perform a second encryption with a different keyword, `STRIPE`, which gives the permutation "564231":

```
5 6 4 2 3 1
E V L N A C
D T E S E A
R O F O D E
E C W I R E
E
```

As before, this is read off columnwise to give the ciphertext:

```
CAEEN SOIAE DRLEF WEDRE EVTOC
```

If multiple messages of exactly the same length are encrypted using the same keys, they can be anagrammed simultaneously. This can lead to both recovery of the messages, and to recovery of the keys (so that every other message sent with those keys can be read).

During World War I, the German military used a double columnar transposition cipher, changing the keys infrequently. The system was regularly solved by the French, naming it Übchi, who were typically able to quickly find the keys once they'd intercepted a number of messages of the same length, which generally took only a few days. However, the French success became widely known and, after a publication in *Le Matin*, the Germans changed to a new system on 18 November 1914.[3]

During World War II, the double transposition cipher was used by Dutch Resistance groups, the French Maquis and the British Special Operations Executive (SOE), which was in charge of managing underground activities in Europe.[4] It was also used by agents of the American Office of Strategic Services[5] and as an emergency cipher for the German Army and Navy.

Until the invention of the VIC cipher, double transposition was generally regarded as the most complicated cipher that an agent could operate reliably under difficult field conditions.

Cryptanalysis

The double transposition cipher can be treated as a single transposition with a key as long as the product of the lengths of the two keys.[6]

In late 2013, a double transposition challenge, regarded by its author as undecipherable, was solved by George Lasry using a divide-and-conquer approach where each transposition was attacked individually.[7]

Myszkowski transposition

A variant form of columnar transposition, proposed by Émile Victor Théodore Myszkowski in 1902, requires a keyword with recurrent letters. In usual practice, subsequent occurrences of a keyword letter are treated as if the next letter in alphabetical order, *e.g.*, the keyword TOMATO yields a numeric keystring of "532164."

In Myszkowski transposition, recurrent keyword letters are numbered identically, TOMATO yielding a keystring of "432143."

```
4 3 2 1 4 3
W E A R E D
```

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

Plaintext columns with unique numbers are transcribed downward; those with recurring numbers are transcribed left to right:

```
ROFOA CDTED SEEEA CWEIV RLENE
```

Disrupted transposition

A disrupted transposition cipher[8] further complicates the transposition pattern with irregular filling of the rows of the matrix, i.e. with some spaces intentionally left blank (or blackened out like in the Rasterschlüssel 44), or filled later with either another part of the plaintext or random letters.[8]

Comb approach

This method (attributed to Gen. Luigi Sacco[9]) starts a new row once the plaintext reaches a column whose key number is equal to the current row number. This produces irregular row lengths. For example,

```
F  O  R  E  V  E  R  J  I  G  S  A  W     < Key
4  8  9  2 12  3 10  7  6  5 11  1 13     Blanks after no.:
C  O  M  P  L  I  C  A  T  E  S  T  *     1
H  E  T  R  *  *  *  *  *  *  *  *  *     2
A  N  S  P  O  S  *  *  *  *  *  *  *     3
I  *  *  *  *  *  *  *  *  *  *  *  *     4
T  I  O  N  P  A  T  T  E  R  *  *  *     5
N  L  I  K  E  A  C  O  M  *  *  *  *     6
B  _  _  _  _  _  _  _  *  *  *  *  *     7
```

The columns are then taken off as per regular columnar transposition: TPRPN, KISAA, CHAIT, NBERT, EMATO, etc.

Numerical sequence approach

Another simple option[10] would be to use a password that places blanks according to its number sequence. E.g. "SECRET" would be decoded to a sequence of "5,2,1,4,3,6" and cross out the 5th field of the matrix, then count again and cross out the second field, etc. The following example would be a matrix set up for columnar transposition with the columnar key "CRYPTO" and filled with crossed out fields according to the disruption key "SECRET" (marked with an asterisk), whereafter the message "we are discovered, flee at once" is placed in the leftover spaces. The resulting ciphertext (the columns read according to the transposition key) is "WCEEO ERET RIVFC EODN SELE ADA".

```
C R Y P T O
1 4 6 3 5 2
W E A R * E
* * D I S *
C O * V E R
E D * F L E
```

```
E * A * * T
O N * C E *
```

Grilles

Another form of transposition cipher uses *grilles*, or physical masks with cut-outs. This can produce a highly irregular transposition over the period specified by the size of the grille, but requires the correspondents to keep a physical key secret. Grilles were first proposed in 1550, and were still in military use for the first few months of World War One.

Detection and cryptanalysis

Since transposition does not affect the frequency of individual symbols, simple transposition can be easily detected by the cryptanalyst by doing a frequency count. If the ciphertext exhibits a frequency distribution very similar to plaintext, it is most likely a transposition.

In general, transposition methods are vulnerable to anagramming—sliding pieces of ciphertext around, then looking for sections that look like anagrams of words in English or whatever language the plaintext was written in, and solving the anagrams. Once such anagrams have been found, they reveal information about the transposition pattern, and can consequently be extended. Simpler transpositions often suffer from the property that keys very close to the correct key will reveal long sections of legible plaintext interspersed by gibberish. Consequently, such ciphers may be vulnerable to optimum seeking algorithms such as genetic algorithms[11] and hill-climbing algorithms.[12][13]

There are several specific methods for attacking messages encoded using a transposition cipher. These include:

1. **Known-plaintext attack:** Using known or guessed parts of the plaintext (e.g. names, places, dates, numbers, phrases) to assist in reverse-engineering the likely order of columns used to carry out the transposition and/or the likely topic of the plaintext.
2. **Brute-force attack:** If keys are derived from dictionary words or phrases from books or other publicly available sources, it may be possible to brute-force the solution by attempting billions of possible words, word combinations, and phrases as keys.
3. **Depth attack:** If two or more messages of the same length are encoded with the same keys, the messages can be aligned and anagrammed until the messages show meaningful text in the same places, without needing to know the transposition steps that have taken place.
4. **Statistical attack:** Statistics about the frequency of 2-letter, 3-letter, etc. combinations in a language can be used to inform a scoring function in an algorithm that gradually reverses possible transpositions based on which changes would produce the most likely combinations. For example, the 2-letter pair QU is more common than QT in English text, so a cryptanalyst will attempt transpositions that place QU together.

The third method was developed in 1878 by mathematician Edward S. Holden and New-York Tribune journalists John R. G. Hassard and William M. Grosvenor who managed to decipher telegrams between the Democratic Party and their operatives in the Southern states during the 1876 presidential election and thus prove facts of vote buying, influencing the 1878-1879 congressional elections.[14]

A detailed description of the cryptanalysis of a German transposition cipher can be found in chapter 7 of Herbert Yardley's "The American Black Chamber."

A cipher used by the Zodiac Killer, called "Z-340", organized into triangular sections with substitution of 63 different symbols for the letters and diagonal "knight move" transposition, remained unsolved for over 51 years, until an international team of private citizens cracked it on December 5, 2020, using specialized software.[15]

Combinations

Transposition is often combined with other techniques such as evaluation methods. For example, a simple substitution cipher combined with a columnar transposition avoids the weakness of both. Replacing high frequency ciphertext symbols with high frequency plaintext letters does not reveal chunks of plaintext because of the transposition. Anagramming the transposition does not work because of the substitution. The technique is particularly powerful if combined with fractionation (see below). A disadvantage is that such ciphers are considerably more laborious and error prone than simpler ciphers.

Fractionation

Transposition is particularly effective when employed with fractionation – that is, a preliminary stage that divides each plaintext symbol into two or more ciphertext symbols. For example, the plaintext alphabet could be written out in a grid, and every letter in the message replaced by its co-ordinates (see Polybius square and Straddling checkerboard).[16] Another method of fractionation is to simply convert the message to Morse code, with a symbol for spaces as well as dots and dashes.[17]

When such a fractionated message is transposed, the components of individual letters become widely separated in the message, thus achieving Claude E. Shannon's diffusion. Examples of ciphers that combine fractionation and transposition include the bifid cipher, the trifid cipher, the ADFGVX cipher and the VIC cipher.

Another choice would be to replace each letter with its binary representation, transpose that, and then convert the new binary string into the corresponding ASCII characters. Looping the scrambling process on the binary string multiple times before changing it into ASCII characters would likely make it harder to break. Many modern block ciphers use more complex forms of transposition related to this simple idea.

See also

- Substitution cipher
- Ban (unit)
- Topics in cryptography

Notes

1. Elonka, Dunin; Schmeh, Klaus (2020). *Codebreaking: A Practical Guide* (http://worldcat.org/

oclc/1158165142). Robinson. p. 247. ISBN 978-1-4721-4421-8. OCLC 1158165142 (https://search.worldcat.org/oclc/1158165142).
2. Smith, Laurence Dwight (1955) [1943], *Cryptography / The Science of Secret Writing*, New York: Dover, pp. 16, 92–93
3. Kahn, pp. 301-304.
4. Kahn, pp. 535 and 539.
5. Kahn, p. 539.
6. Barker, Wayne (1995). *Cryptanalysis of the Double Transposition Cipher: Includes Problems and Computer Programs*. Aegean Park Press.
7. Lasry, George (2014-06-13). "Solving the Double Transposition Challenge with a Divide-and-Conquer Approach". *Cryptologia*. **38** (3): 197–214. doi:10.1080/01611194.2014.915269 (https://doi.org/10.1080%2F01611194.2014.915269). S2CID 7946904 (https://api.semanticscholar.org/CorpusID:7946904).
8. Mahalakshmi, B. (June 2016). "An Overview on Disrupted Transposition Cipher for Security Enhancement" (https://www.ijcaonline.org/archives/volume143/number13/mahalakshmi-2016-ijca-910308.pdf) (PDF). *International Journal of Computer Applications*. **143** (13): 9–12. doi:10.5120/ijca2016910308 (https://doi.org/10.5120%2Fijca2016910308). Archived (https://web.archive.org/web/20180604051237/http://www.ijcaonline.org/archives/volume143/number13/mahalakshmi-2016-ijca-910308.pdf) (PDF) from the original on 2018-06-04. Retrieved 7 January 2021.
9. Savard, John. "Methods of Transposition" (http://www.quadibloc.com/crypto/pp0102.htm). *A Cryptographic Compendium*. Retrieved 27 June 2023.
10. jdege (11 November 2014). "A simple disrupted transposition" (https://www.tapatalk.com/groups/crypto/a-simple-disrupted-transposition-t1074.html). Retrieved 7 January 2021.
11. Matthews, Robert A. J. (April 1993). "The Use of Genetic Algorithms in Cryptanalysis". *Cryptologia*. **17** (2): 187–201. doi:10.1080/0161-119391867863 (https://doi.org/10.1080%2F0161-119391867863).
12. Lasry, George; Kopal, Nils; Wacker, Arno (2014-07-03). "Solving the Double Transposition Challenge with a Divide-and-Conquer Approach" (http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.915269). *Cryptologia*. **38** (3): 197–214. doi:10.1080/01611194.2014.915269 (https://doi.org/10.1080%2F01611194.2014.915269). ISSN 0161-1194 (https://search.worldcat.org/issn/0161-1194). S2CID 7946904 (https://api.semanticscholar.org/CorpusID:7946904).
13. Lasry, George; Kopal, Nils; Wacker, Arno (2016-07-03). "Cryptanalysis of columnar transposition cipher with long keys" (http://www.tandfonline.com/doi/full/10.1080/01611194.2015.1087074). *Cryptologia*. **40** (4): 374–398. doi:10.1080/01611194.2015.1087074 (https://doi.org/10.1080%2F01611194.2015.1087074). ISSN 0161-1194 (https://search.worldcat.org/issn/0161-1194). S2CID 21179886 (https://api.semanticscholar.org/CorpusID:21179886).
14. "[3.0] The Rise Of Field Ciphers" (https://vc.airvectors.net/ttcode_03.html#m3). *vc.airvectors.net*. Retrieved 2024-01-11.
15. "Zodiac Killer cipher is cracked after eluding sleuths for 51 years" (https://arstechnica.com/information-technology/2020/12/zodiac-killer-cipher-is-cracked-after-eluding-sleuths-for-51-years/). *arstechnica.com*. 2020-12-12. Retrieved 2020-12-12.
16. Daniel Rodriguez-Clark. "Transposing Fractionated Ciphertext" (https://crypto.interactive-maths.com/transposing-fractionated-text.html).
17. James Lyons. "Fractionated Morse Cipher" (http://practicalcryptography.com/ciphers/classical-era/fractionated-morse/).

References

- Kahn, David. The Codebreakers: The Story of Secret Writing. Rev Sub. Scribner, 1996.
- Yardley, Herbert. The American Black Chamber. Bobbs-Merrill, 1931.
