Columnar Ciphers: Everything you need to know

By Shreya Shukla

What is a transposition cipher?

A transposition cipher is when plaintext is simply rearranged to create a permutation. It is done by arranging letters in a grid, and changing the order in which they are read as text.

This is different from a substitution cipher, where the letters in plaintext are replaced to create ciphertext.

A double transposition cipher involves using a keyword and applying the transposition. Such a cipher is called a Columnar Cipher, and is relatively hard to break in comparison to other ciphers.

Brief history

Columnar Cipher has been used for decades, going back to World War 1, where it was used the Germans to communicate with armies. Since then, it has been used by British intelligence, the NSA, the CIA, WW2 American Army, etc.

In 1999, it was published by Otto Leibrich, a German information security government official, to encourage research on the topic.

This cipher was preferred to others because it does not require a device to encrypt text.

It can simply be done manually, and up until a couple years ago, it was thought to be unbreakable.

How does the double transposition cipher work?

T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

TINESAX
EOAHTFX
HTLTHEY
MAIIAIX
TAPNGDL
OSTNHMX

1) Index your keyword based on the alphabet (TOMATO -> 532164)
2) Create a grid of n columns 3) Write your plaintext by rows
4) Scramble your grid based on the numerical order of the column indices (532164 -> 123456)
5) Read your grid by rows
THIS IS YOUR CIPHERTEXT!

How to break the Columnar Cipher?

1) Brute Force Attack: Try all combinations of keywords < 9.

2) Dictionary Attack: Try all common words from a dictionary

3) Hill-climbing cipher: assume key-length and try permutations of alphabet with key-length

-> can take all night to work

-> inefficient because it would just be easier to run combinations of key indices

-> does not work if you use two different keywords (you can use two keywords to encrypt code twice)

What I did (mix of brute force and dictionary attack)

I decrypted the columnar cipher after reading online that it could be broken using dictionary attacks. I simply wrote a decrypt function, and ran it for permutations of a given key length. (for a given number n, PnR = n!/(n-r)! or in this case PnR = n!)

There are probably other more successful techniques to break this cipher, but this works efficiently. Even if you don't get the correct answer on your first try, you will eventually get the right answer. Although, if you know the key_length, you should get the answer on the first try.

(Code on GitHub)

Sources used:

Research Paper:
https://www.uni-kassel.de/eecs/fileadmin/datas/fb16/Fachgebiete/UC/papers/Solving_the_Double_Transposition_Challenge_with_a_Divide_and_Conquer_Approach.pdf

Algorithm:

http://www.counton.org/explorer/codebreaking/transposition-ciphers.php

Wiki:

https://en.wikipedia.org/wiki/Transposition_cipher#:~:text=In%20cryptography%2C%20a%20transposition%20cipher,a%20permutation%20of%20the%20plaintext.

Army:

https://stationhypo.com/2018/11/11/americas-first-code-breakers-how-the-u-s-military-helped-win-the-ww1-intelligence-war-guest-post/