TWO ATTACKS ON TABLEAU-BASED CIPHERS

Two attacks on tableau-based ciphers

madness
2020-09-20

What do we mean by “tableau-based” cipher? By that we mean any periodic polyalphabetic substitution cipher all of whose key alphabets are known to the attacker and can be tabulated. The first cipher that should come to your mind is the Vigenère cipher and its table, the “tabula recta.” But there are others: Beaufort, variant (German) Beaufort, Gronsfeld, Porta (two versions), and the recently discovered Bellaso 1552 cipher. We assume that you already know how to use the tableau for the Vigenère cipher; the others function the same way. In the tables at the end of this document are the tableaux for these six ciphers.

Finding the period

The first thing we must do is find the period of the cipher, which is also the length of the key. We can do it the hard way with the Kasiski method, or we can automate it using the index of coincidence or the twist/twist+ method. Or we can just guess. The algorithms that we describe below are fast enough that we can try each value for the period until we get an acceptable result. There are some excellent references at the end of this document, if you would like to automate the determination of the period.

Frequency-matching attack

Our first attack is an automation and generalization of an old attack on the Vigenère cipher. We cut a ciphertext into slices. If the period is m, then the n^{th} slice consists of every m^{th} letter, beginning with the n^{th}. So the first slice will contain the first letter of the ciphertext, the $(m+1)^{\text{st}}$ letter, the $(2m+1)^{\text{st}}$ letter, etc.; the second slice contains the second letter, the $(m+2)^{\text{nd}}$ letter, etc. For each slice, we decipher it with every possible single-letter key. For each decipherment, we compare the monogram (single-letter) frequencies of the result with the monogram frequencies of English. The key letter that gives the best fit is kept as a character in the cipher’s key.

To compare two sets of frequencies, we prefer the inner vector product rather than the χ^2 (chi-squared) statistic. The χ^2 statistic has the expected values in the denominator of each term. For less frequent letters, such as ‘J’ or ‘X,’ a small increase in their use in the plaintext can lead to a large χ^2 and give us the wrong result. The inner vector product is not susceptible to this error. The inner product, often called the “dot” product because it is written with a bold dot between two vectors, is quite simple. Suppose we have two vectors, which are really just ordered lists of numbers with length L, $\mathbf{x} = \{x_1, x_2, x_3, ..., x_L\}$ and $\mathbf{y} = \{y_1, y_2, y_3, ..., y_L\}$. The inner product of $\mathbf{x}$ and $\mathbf{y}$ is the sum of the products of those numbers:

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{L} x_i y_i$$

The algorithm for the attack is as follows:

1. Slice the ciphertext *c* as described above
2. Set the key *K* to be an empty list of characters
3. For *i* in 1, ..., *m* (the period):
    a. Set the best value of the dot product *D* to zero
    b. For all possible single characters *a* that can appear in the key:
        i. Decipher the i^{th} slice of *c*, using *a* as the key, to obtain a plaintext *p*
        ii. Calculate the list of monogram frequencies f_p for *p*
        iii. Calculate the dot product *d* of f_p and English frequencies f_E
        iv. If $d > D$:
            - Set *D* equal to *d*
            - Set the current key character *k* to *a*
    c. Append *k* to *K*
4. Output the key *K*

There is a list of monogram frequencies for English in the last table of this document. It was calculated from the Brown University corpus of English text. Feel free to use it.

Hill-climbing attack

For this attack we need a way of judging how close a text resembles English. For this we like to use what we call tetragram (four-letter) fitness. Unfortunately, a table of tetragrams and their frequencies would be far too large to put in this tiny document, so you will have to generate your own. If we have a text $T=\{t_1, t_2, t_3, ..., t_L\}$ of length *L*, the fitness *F* is calculated as an average logarithm of the English frequencies f_E of the tetratrams that appear in *T*:

$$F = \frac{1}{L-3} \sum_{i=1}^{L-3} \log\left(\max\left[f_E(t_i, t_{i+1}, t_{i+2}, t_{i+3}), \varepsilon\right]\right)$$

We need to use the maximum of the frequency and some small number ε so that we do not run into any mathematical errors when we encounter a frequency that is zero.

The attack seeks to maximize the fitness of the deciphered text. First, it tries all possibilities for the first character in the key and chooses the one that gives the best fitness. Then it tries all possibilities for the second character in the key. Then the third. It runs through each position in the key. Then it returns to the first position again. This continues until it tries to modify each character in the key but cannot increase the fitness any longer.

Here is the algorithm for this attack:

1. Set the key K to be a list of any key characters; the length of the list is the period m
2. Set the fitness F to a large negative number, such as −100
3. Loop:
    a. Set a temporary variable F_{old} equal to F
    b. For i in 1, ..., m:
        i. Copy K into a temporary key k
        ii. Set the best key character b equal to the i^{th} character of K
        iii. Set a temporary maximum fitness f_{max} equal to F
        iv. For all possible characters a that can appear in a key:
            - Set the i^{th} character of k equal to a
            - Decipher the ciphertext c with the key k to obtain a plaintext p
            - Calculate the fitness f of p
            - If $f > f_{max}$:
                - Set f_{max} equal to f
                - Set b equal to a
        v. Set the i^{th} character of K equal to b
        vi. Set F equal to f_{max}
    c. If F equals F_{old}, then exit the loop and go to step 4
4. Output the key K

You will find that this attack is quite good at recovering the key, often even for a ciphertext that is as short as ten periods. For such a short ciphertext, it may be necessary to guess at the value of the period, since there are not enough characters to do the required statistics to find the period with the index of coincidence or the twist method.

References

American Cryptogram Association, The ACA and You, 2005, www.cryptogram.org/downloads/aca.info/ciphers/Beaufort.pdf, www.cryptogram.org/downloads/aca.info/ciphers/Gronsfeld.pdf, www.cryptogram.org/downloads/aca.info/ciphers/Variant.pdf, www.cryptogram.org/downloads/aca.info/ciphers/Vigenere.pdf, web.archive.org/web/*/www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf

Thomas H. Barr and Andrew J. Simoson, "Twisting the Keyword Length from a Vigenère Cipher," *Cryptologia* 39:4 (2015) 335-341, DOI: 10.1080/01611194.2014.988365

Giovan Battista Bellaso, *La Cifra del Sig. Giouan Battista Bellaso*, 1553.

Paolo Bonavoglia, "Bellaso's 1552 cipher recovered in Venice," *Cryptologia* 43:6 (2019) 459-465, DOI: 10.1080/01611194.2019.1596181

Paolo Bonavoglia, "Trithemius, Bellaso, Vigenère: Origins of the Polyalphabetic Ciphers," Proceedings of the 3rd International Conference on Historical Cryptology, 2020, ep.liu.se/ecp/171/007/ecp2020_171_007.pdf, DOI: 10.3384/ecp2020171007

Brown University, Brown Corpus Manual, 1979, http://listings.lib.msu.edu/public-corpora/cd421/manuals/brown/INDEX.HTM

Augusto Buonafalce, "Bellaso's Reciprocal Ciphers," *Cryptologia* 30:1 (2006) 39-51, DOI: 10.1080/01611190500383581

William F. Friedman, The Index of Coincidence and Its Applications in Cryptography, Riverbank Laboratories Department of Ciphers Publication 22, Geneva, Illinois, 1920, www.marshallfoundation.org/library/methods-solution-ciphers

Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; http://archive.org/details/cryptanalysis00gain

Friedrich Kasiski, *Die Geheimschriften und die Dechiffrir-Kunst*, 1863, digital.onb.ac.at/OnbViewer/viewer.faces?doc=ABO_+Z224431001

James Lyons, "Cryptanalysis of the Vigenere Cipher," Practical Cryptography, 2012, practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher

James Lyons, "Cryptanalysis of the Vigenere Cipher, Part 2," Practical Cryptography, 2012, practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher-part-2

James Lyons, "Quadgram Statistics as a Fitness Measure," Practical Cryptography, 2012, practicalcryptography.com/cryptanalysis/text-characterisation/quadgrams

Marjorie Mountjoy, "The bar statistics," *NSA Technical Journal* VII (2, 4), 1963.

Seongmin Park, Juneyeun Kim, Kookrae Cho, and Dae Hyun Yum, “Finding the key length of a Vigenère cipher: How to improve the twist algorithm,” *Cryptologia* 44:3 (2020) 197-204, DOI: 10.1080/01611194.2019.1657202

Johannes Trithemius, *Polygraphiae libri sex*, Reichenau: Joannis Haselberg de Aia, 1518, www.loc.gov/item/32017914

Blaise de Vigenère, *Traicté des chiffres ou secrètes manières d’escrire*, Paris: Abel l’Angelier, 1586, HDL: 2027/ien.35552000251008, gallica.bnf.fr/ark:/12148/bpt6k1040608n, gallica.bnf.fr/ark:/12148/bpt6k94009991

Table 1: Tableau for the modern version of the Vigenère cipher.

key	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Table 2: Tableau for the Gronsfeld cipher. These are the first ten rows of the Vigenère tableau.

key	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
0	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
8	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
9	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

Table 3: Tableau for the Beaufort cipher.

key	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
A	A Z Y X W V U T S R Q P O N M L K J I H G F E D C B
B	B A Z Y X W V U T S R Q P O N M L K J I H G F E D C
C	C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
D	D C B A Z Y X W V U T S R Q P O N M L K J I H G F E
E	E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
F	F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
G	G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
H	H G F E D C B A Z Y X W V U T S R Q P O N M L K J I
I	I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
J	J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
K	K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
L	L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
M	M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
N	N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
O	O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
P	P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
Q	Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
R	R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
S	S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
T	T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
U	U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
V	V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
W	W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
X	X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
Y	Y X W V U T S R Q P O N M L K J I H G F E D C B A Z
Z	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Table 4: Tableau for the variant (German) Beaufort cipher.

key	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
C	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
D	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
E	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
F	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
G	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
H	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
I	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
J	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
K	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
L	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
M	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
P	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
Q	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
R	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
S	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
T	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
U	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
V	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
W	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
X	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Y	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
Z	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Table 5: Tableau for the modern Porta cipher. There are two versions in common use.

key (version)		plaintext alphabet
1	2	a b c d e f g h i j k l m n o p q r s t u v w x y z
A/B	A/B	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
C/D	Y/Z	O P Q R S T U V W X Y Z N M A B C D E F G H I J K L
E/F	W/X	P Q R S T U V W X Y Z N O L M A B C D E F G H I J K
G/H	U/V	Q R S T U V W X Y Z N O P K L M A B C D E F G H I J
I/J	S/T	R S T U V W X Y Z N O P Q J K L M A B C D E F G H I
K/L	Q/R	S T U V W X Y Z N O P Q R I J K L M A B C D E F G H
M/N	O/P	T U V W X Y Z N O P Q R S H I J K L M A B C D E F G
O/P	M/N	U V W X Y Z N O P Q R S T G H I J K L M A B C D E F
Q/R	K/L	V W X Y Z N O P Q R S T U F G H I J K L M A B C D E
S/T	I/J	W X Y Z N O P Q R S T U V E F G H I J K L M A B C D
U/V	G/H	X Y Z N O P Q R S T U V W D E F G H I J K L M A B C
W/X	E/F	Y Z N O P Q R S T U V W X C D E F G H I J K L M A B
Y/Z	C/D	Z N O P Q R S T U V W X Y B C D E F G H I J K L M A

Table 6: Tableau for a modernized version of the Bellaso 1552 cipher.

key	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
A	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
B	Z N O P Q R S T U V W X Y B C D E F G H I J K L M A
C	Y Z N O P Q R S T U V W X C D E F G H I J K L M A B
D	X Y Z N O P Q R S T U V W D E F G H I J K L M A B C
E	W X Y Z N O P Q R S T U V E F G H I J K L M A B C D
F	V W X Y Z N O P Q R S T U F G H I J K L M A B C D E
G	U V W X Y Z N O P Q R S T G H I J K L M A B C D E F
H	T U V W X Y Z N O P Q R S H I J K L M A B C D E F G
I	S T U V W X Y Z N O P Q R I J K L M A B C D E F G H
J	R S T U V W X Y Z N O P Q J K L M A B C D E F G H I
K	Q R S T U V W X Y Z N O P K L M A B C D E F G H I J
L	P Q R S T U V W X Y Z N O L M A B C D E F G H I J K
M	O P Q R S T U V W X Y Z N M A B C D E F G H I J K L
N	M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
O	A M L K J I H G F E D C B Y X W V U T S R Q P O N Z
P	B A M L K J I H G F E D C X W V U T S R Q P O N Z Y
Q	C B A M L K J I H G F E D W V U T S R Q P O N Z Y X
R	D C B A M L K J I H G F E V U T S R Q P O N Z Y X W
S	E D C B A M L K J I H G F U T S R Q P O N Z Y X W V
T	F E D C B A M L K J I H G T S R Q P O N Z Y X W V U
U	G F E D C B A M L K J I H S R Q P O N Z Y X W V U T
V	H G F E D C B A M L K J I R Q P O N Z Y X W V U T S
W	I H G F E D C B A M L K J Q P O N Z Y X W V U T S R
X	J I H G F E D C B A M L K P O N Z Y X W V U T S R Q
Y	K J I H G F E D C B A M L O N Z Y X W V U T S R Q P
Z	L K J I H G F E D C B A M N Z Y X W V U T S R Q P O

Table 7: Monogram frequencies for English. Obtained from the Brown University corpus of English text.

A	0.0804
B	0.0153
C	0.0311
D	0.0396
E	0.1250
F	0.0234
G	0.0195
H	0.0541
I	0.0730
J	0.0016
K	0.0066
L	0.0413
M	0.0254
N	0.0710
O	0.0760
P	0.0202
Q	0.0011
R	0.0614
S	0.0655
T	0.0925
U	0.0271
V	0.0100
W	0.0188
X	0.0020
Y	0.0172
Z	0.0010

Test ciphertexts

Despite the shortness of these ciphertexts, you should be able to break them with both of the attacks described in this document.

```
MLEGENTQTXAQLVLCMSUIUEWCKETGEVBLYVOCTFYRAIHDUJXYGHTWEDTPVLHPRVTLWXHTH
RMRXVWTRVAYOMNVTVTYMMTPDFKKHYSTWRLQBXTXNXUCMAETNKACFJAHTRLJXIPPNUMFXS
TWEIMUHAEGELLGGKIIAJTANWHXOEKCLXICGKACBVEABFPQHRIIAEWRTPKXNXHTXVIISYX
YW

DUNVPJSUQWCZDBFTEPUJWKRPQAZUMGNRZWEQDTUFMUYYCKWZKUNZXHMRZREQKGFQXKSHG
FULUNWESTLBTNSVDVKWVVYA

NNNNNSTQIZETSOOHNQAGHKHWNQEZPQNEBPIFCWXWEZAPNZTVIFUPDPEBDJGKBURPWAXIR
RAXBYEQJWIRGHSHYRCBYRANGPETNNHQVSJCKDFNINHLVPIFESCZLMCHQRDSTZNDKDUVEW
WCNDASNPMCWZ

LPFWGYOQZWEYMPJQBUAAABERNHILAEVILPFLMETWHETXTVQEBPIWAAZEBYERNREBQXIMA
BMLMIRAGUMRBMINBAHGFOCRPMTWHEMMXEBTTQEBFKYKXUSTQVTLTXCESUSLXIULLVGWAA
JQGPCRFMQXTPOQZWIEGUHCFOVMPKYKQUZLLFMNPQMGVUSRPNINPNIRBTYUPPYLLWI

HTKLKFYUCOSTGLYZAYMZWFYMUSEHGPVUYBEAQGVZKMYOKWZMWBTUTBKOPUHAPGZWJPQOV
CDUTKDSPHGPVQNIPHQXQPKAQMQDMMIEBIOBDOXOBPZQYPNWQQBDWEVQAQQUNNIPKVAGEC
IOAAXMPVMTIHWOKKKIXJJAODYPAUAZCLWZMZAOFJQOUGYBWBPCIHYQJWBTFNMZCDSWQGQ
LMHZMYTASBOVOHMTBHM
```