Fall 2006
Chris Christensen
MAT/CSC 483

Gronsfeld Cipher and Beaufort Cipher

The telegraph was invented by Samuel Morse in 1844, and it revolutionized communications. For the first time, it became possible to instantly transmit messages over long distances. Military commanders could now gather information from and send commands to armies in the field. It was also possible to quickly transmit commercial and private communications over long distances. But, as with any new communication system, there were problems of secrecy. Clearly, the telegraph operators at the sending and at the receiving end of the message could read it unless it were encrypted, and it was possible for eavesdroppers to tap telegraph lines and intercept the messages that were being transmitted.

> As the most exciting invention of the first half of the [Nineteenth] century, the telegraph stirred as much interest in its day as Sputnik did in [the mid-Twentieth Century]. The great and widely felt need for secrecy awakened the latent interest in ciphers that so many people seem to have, and kindled a new interest in many others. Dozens of persons tried to dream up their own unbreakable ciphers. Nearly all were amateurs, the professionals (except for a few code clerks) having lost their jobs when the black chambers [which flourished from the early Seventeenth until the mid Nineteenth Century] were abolished. A surprising number of these dabblers were intellectual and political leaders of the day who beamed their powerful and original minds on the engrossing field of cryptology. Their contributions enriched it with dozens of new cipher systems. (*The Codebreakers* by David Kahn)

Gronsfeld Cipher

In 1892, French authorities arrested a group of anarchists and brought them to trial. Included in the evidence was a number of cryptograms that had been solved by [Étienne] Bazeries [1846 – 1931]. They used a system called the Gronsfeld, a kind of truncated Vigenère named for the count of Gronsfeld. Its key consists of numbers, each of which indicates the number of letters forward in the normal alphabet that the encipherer is to count from the plaintext letter to the ciphertext letter. (*The Code Breakers* by David Kahn)

Here is a table for the Gronsfeld cipher.

abcdefghijklmnopqrstuvwxyz
0ABCDEFGHIJKLMNOPQRSTUVWXYZ
1BCDEFGHIJKLMNOPQRSTUVWXYZA
2CDEFGHIJKLMNOPQRSTUVWXYZAB
3DEFGHIJKLMNOPQRSTUVWXYZABC
4EFGHIJKLMNOPQRSTUVWXYZABCD
5FGHIJKLMNOPQRSTUVWXYZABCDE
6GHIJKLMNOPQRSTUVWXYZABCDEF
7HIJKLMNOPQRSTUVWXYZABCDEFG
8IJKLMNOPQRSTUVWXYZABCDEFGH
9JKLMNOPQRSTUVWXYZABCDEFGHI

Beaufort Cipher

In England in 1857, a 4×5 card with an alphabet square printed in red and black went on sale for sixpence. It was a new system of secret writing "adapted for telegrams and postcards," the latter an even newer form of communication than the telegraph. Admiral Sir Francis Beaufort, R.N., creator of the Beaufort scale with which meteorologists indicate wind velocity …, had originated the cipher, and his brother published it a few months after the admiral's death. … The alphabet square is essentially the same as Vigenère, except that it repeats the normal alphabet on all four sides … . Its [method of] encipherment equals that of a Vigenère with reversed alphabets. … The envelope for the card carried the instructions: "Let the key for the foregoing table be a line of poetry or the name of some memorable person or place, which cannot easily be forgotten … . Now look in the side column [either side column] for the first letter of the [plain]text (*t*) and run the eye across the table until it comes to the first letter of the key (*v*), then at the top of the column in which v stands will be found the letter c, " which would be the ciphertext. (*The Code Breakers* by David Kahn)

The Original Beaufort Square

```
ABCDEFGHIJKLMNOPQRSTUVWXYZA
BCDEFGHIJKLMNOPQRSTUVWXYZAB
CDEFGHIJKLMNOPQRSTUVWXYZABC
DEFGHIJKLMNOPQRSTUVWXYZABCD
EFGHIJKLMNOPQRSTUVWXYZABCDE
FGHIJKLMNOPQRSTUVWXYZABCDEF
GHIJKLMNOPQRSTUVWXYZABCDEFG
HIJKLMNOPQRSTUVWXYZABCDEFGH
IJKLMNOPQRSTUVWXYZABCDEFGHI
JKLMNOPQRSTUVWXYZABCDEFGHIJ
KLMNOPQRSTUVWXYZABCDEFGHIJK
LMNOPQRSTUVWXYZABCDEFGHIJKL
MNOPQRSTUVWXYZABCDEFGHIJKLM
NOPQRSTUVWXYZABCDEFGHIJKLMN
OPQRSTUVWXYZABCDEFGHIJKLMNO
PQRSTUVWXYZABCDEFGHIJKLMNOP
QRSTUVWXYZABCDEFGHIJKLMNOPQ
RSTUVWXYZABCDEFGHIJKLMNOPQR
STUVWXYZABCDEFGHIJKLMNOPQRS
TUVWXYZABCDEFGHIJKLMNOPQRST
UVWXYZABCDEFGHIJKLMNOPQRSTU
VWXYZABCDEFGHIJKLMNOPQRSTUV
WXYZABCDEFGHIJKLMNOPQRSTUVW
XYZABCDEFGHIJKLMNOPQRSTUVWX
YZABCDEFGHIJKLMNOPQRSTUVWXY
ZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZA
```

Here is another example using the original square: Let us encrypt the letter h with key F. Find the plaintext letter h in the column on the left or on the right. Find in that row the key F. Proceed up that column to the ciphertext letter in the top row Y (or down the column to the ciphertext Y in the bottom row).

Notice that the Beaufort encryption is reciprocal. Begin with ciphertext Y. Find Y in the column on the left or on the right. Find in that row the key F. Proceed up that column to the plaintext letter in the top row h.

Also, try encrypting h with key F using the Vigenère rules and the Vigenère square with reversed alphabets.

Vigenère square with reversed alphabets

abcdefghijklmnopqrstuvwxyz
ZYXWVUTSRQPONMLKJIHGFEDCBA
AZYXWVUTSRQPONMLKJIHGFEDCB
BAZYXWVUTSRQPONMLKJIHGFEDC
CBAZYXWVUTSRQPONMLKJIHGFED
DCBAZYXWVUTSRQPONMLKJIHGFE
EDCBAZYXWVUTSRQPONMLKJIHGF
FEDCBAZYXWVUTSRQPONMLKJIHG
GFEDCBAZYXWVUTSRQPONMLKJIH
HGFEDCBAZYXWVUTSRQPONMLKJI
IHGFEDCBAZYXWVUTSRQPONMLKJ
JIHGFEDCBAZYXWVUTSRQPONMLK
KJIHGFEDCBAZYXWVUTSRQPONML
LKJIHGFEDCBAZYXWVUTSRQPONM
MLKJIHGFEDCBAZYXWVUTSRQPON
NMLKJIHGFEDCBAZYXWVUTSRQPO
ONMLKJIHGFEDCBAZYXWVUTSRQP
PONMLKJIHGFEDCBAZYXWVUTSRQ
QPONMLKJIHGFEDCBAZYXWVUTSR
RQPONMLKJIHGFEDCBAZYXWVUTS
SRQPONMLKJIHGFEDCBAZYXWVUT
TSRQPONMLKJIHGFEDCBAZYXWVU
UTSRQPONMLKJIHGFEDCBAZYXWV
VUTSRQPONMLKJIHGFEDCBAZYXW
WVUTSRQPONMLKJIHGFEDCBAZYX
XWVUTSRQPONMLKJIHGFEDCBAZY
YXWVUTSRQPONMLKJIHGFEDCBAZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

[The Beaufort cipher] had originally proposed almost 150 years before Beaufort by one Giovanni Sestri in a book published in Rome in 1710 that had been widely ignored. But under Beaufort's name the cipher became a standard part of the repertory of cryptology, though its theoretical importance in minor.

Variant Beaufort

[The Beaufort cipher] has also given rise to a system called the Variant Beaufort. In this [cipher system], the encipherer starts, not with the plaintext letter but with the keyletter, traces in to the plaintext letter, and then turns upward to emerge at the ciphertext. Actually the system might better be called Variant Vigenère, for to decipher it the clerk must perform the operation that constitutes a Vigenère encipherment: find the keyletter on the side and the ciphertext letter at the top, and run into the tableau from both until the plaintext letter is located at the junction. Vigenère and Variant Beaufort thus invert one another – the encipherment of one serves as the decipherment of the other. True Beaufort, on the other hand, is reciprocal within itself, since the operation of starting with the known letter, tracing in to the keyletter, and rising to find the unknown works for both encipherment and decipherment. (*The Code Breakers* by David Kahn)

Exercises

1. Use a Gronsfeld cipher with key 94382 to encipher the message:

```
The Cardano grille consists of a sheet of stiff
material into which rectangular holes are cut at
irregular intervals.
```

2. Use a Gronsfeld cipher with NKU's Department of Mathematics' phone number 8595725377 as the key to encipher the message:

```
Cardano also achieved the dubious distinction of
being the first cryptologist to cite the enormous
number of variants inherent in cryptographic system
as proof of the impossibility of a cryptanalyst's
ever reaching a solution during his lifetime.
```

3. Describe how you would attack a Gronsfeld cipher.

4. Cryptanalyze the following ciphertext that was enciphered with a Gronsfeld cipher.

```
wpjwg wqtwg oajla uqyhg jmsle zixny wiguo vpjmh
bxwny lljwz liqmo umhco ymfbg vmujx dbjjm hvhhc
lbmrt wpjmk siwcs hvyxl gmknt vmzwj hzyqk gqwni
wqtwg xbmxx lbdjt gktwz uwqxl wpjbk fzjcg ugtoj
hnjwy hemxc dainy losjz hljgk fcyrb hilnt wntaz
kmunx iwwvg qkjxl kqlqr bauni liqrf hlkdt fbnxt
vqsba sxtaz rnyqk lvynr oqlnt fmflz ldnco hatoz
kmzwo wmxbz dbjb
```

$I \approx 0.0426$ and $l \approx 5.8265$. What is the key? Is this easier, harder, or about the same level of difficulty as cryptanalyzing a Vigenère cipher?

5. The plaintext message in exercise 2 contains 208 letters. Use the first 208 digits of the expansion of Pi as needed to encipher the message in exercise 2 using a Gronsfeld cipher. Here are the first 1000 digits of Pi.

```
3.14159265358979323846264338327950288419716939937510582097
49445923078164062862089986280348253421170679821480865132
82306647093844609550582231725359408128481117450284102701
93852110555964462294895493038196442881097566593344612847
56482337867831652712019091456485669234603486104543266482
13393607260249141273724587006606315588174881520920962829
25409171536436789259036001133053054882046652138414695194
15116094330572703657595919530921861173819326117931051185
48074462379962749567351885752724891227938183011949129833
67336244065664308602139494639522473719070217986094370277
05392171762931767523846748184676694051320005681271452635
60827785771342757789609173637178721468440901224953430146
54958537105079227968925892354201995611212902196086403441
81598136297747713099605187072113499999983729780499510597
31732816096318595024459455346908302642522308253344685035
26193118817101000313783875288658753320838142061717766914
73035982534904287554687311595628638823537875937519577818
57780532171226806613001927876611195909216420199
```

6. The digits of Pi are known to form a random string. Keeping that in mind, is it possible to successfully attack the ciphertext that would result from exercise 5?

7. Use a Beaufort cipher with keyword `Vigenere` to encipher the message: `Vigenere was not a nobleman.`

8. Describe how you would attack a Beaufort cipher.