XXX

Dr. Bruff

Math 115-F

2 Nov. 2010

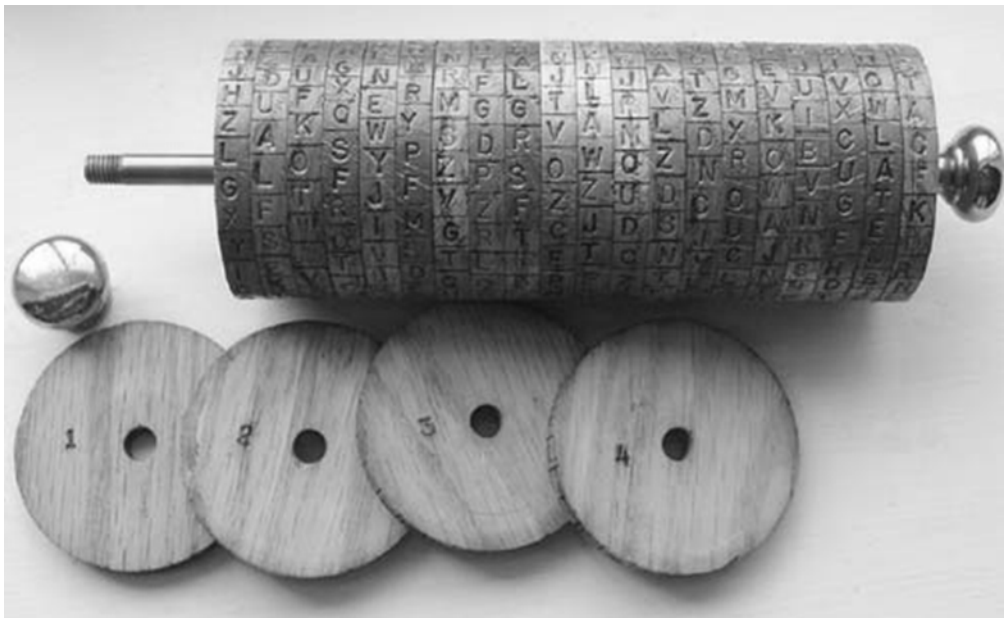
Bazeries Cylinder

Invented by Thomas Jefferson in 1795, the wheel cypher, better known as the Bazeries Cylinder, was one of the first forms of a cryptographic machine. Although reportedly not used by President Jefferson, it represents an ingenuity that was emerging on the cryptographic landscape at the turn of the century. Sandwiching this invention were other discoveries that represented a growing emphasis of technology in society: the telegraph in the late eighteenth century and the Difference Engine #1 in 1823 (Bruff). Although seemingly unrelated, these three innovations show how there was a growing tendency towards technological advancement during this time period. Jefferson's wheel cypher did not gain fame until it was independently reproduced by Commandant Bazeries in the late nineteenth century. It was subsequently used as a military cipher when "Parker Hitt designed a 'strip cipher' that was equivalent to Jefferson's cypher… [which] was used as a U.S. Army field cipher" (Barr) after World War I.

During the time period from 1923 to 1942, the Bazeries Cylinder gained a reputation as one of the best methods of encryption that the United States military possessed. Utilized by many branches, including the Army, Coast Guard, and the FCC this encryption not only improved security of messages, but also evolved and grew more complex. As technology improved, the cylinder was able to be modified, continuing to baffle its would-be crackers. In this way, it is similar to the Vignere Cipher in its ability

to completely puzzle anyone who attempted decryption. The implementation of more individual disks that contained more letters helped ensure its security. In fact, it was deemed safe enough for the US State Department and the United States Navy to use during the early part of World War II (Kahn).

The structure of the Bazeries Cylinder is very basic. A randomized alphabet is printed on the outside edge of a circular disk. Every individual disk is marked as a specific number that indicates which order the letters appear. Each disk is then stacked upon a center, usually iron, axle (Barr). The order in which these disks are stacked as well as the number of disks is up to the discretion of the person who is encrypting the message. These rotatable disks are then free to form whatever message the beholder has as long as the message's length does not exceed the number of disks on the cylinder.



Source: Torrone, Phillip. "Happy President's Day from MAKE." 18 February 2008. MAKE. 30 October 2010 <http://blog.makezine.com/archive/2008/02/happy_presidents_day_from.html>.

The essential part of the decryption of the Bazeries Cylinder rests upon the recipient of the message having the correct order of disks on his or her own cylinder. Once an order had been decided, the writer of the message would record the disks' order numerically and send that to the recipient. They would then rearrange the disks to a desired message and choose a previously specified row of the disks to serve as the cipher text (Goebel). This information would be sent to the message's intended reader as well so that they could use a specific set of letters in reference to the row that contained the actual message. Because the code relied upon information that only the sender and receiver knew, it was generally an effective way of enciphering.

The Bazeries Cylinder was not easily broken due to the fact that even with just ten disks on the axle, you still have 10!, or 3,628,800, possibilities (Goebel). This makes checking each possible arrangement of the disks a near impossible task. However, it is once you are given a few other critical pieces of information that the cylinder's weakness is exposed. One of the main weaknesses is that the cipher text is visible at the same time the actual message is (Goebel). This is due to the fact that all of the possible letters are always visible and once a cipher text is created, the intended message appears as well. Additionally, the cipher text and the message are always the same number of letters apart because in order to see the message, all of the letters must be in line with each other. Therefore, the person doing the encrypting must use a single row to contain the cipher text, resulting in a constant number of rows separating the cipher and message. This greatly aids the decrypting process as it eliminates the need to search every disk for what row contains the cipher. If you are given both the cipher in its encrypted and plaintext form, it is much easier to determine the order that the disks are arranged in.

One of the easiest ways to obtain both of these pieces of information is for the cryptanalyst to discover a crib, or a reoccurring strand of plain text. The crib is often used to help discover the relationship between the plaintext and the cipher. With the cipher text and the crib in hand, the cryptanalyst has the key he needs to crack the cylinder. If the two texts are lined up, one next to the other, corresponding letters can be formed into pairs. For example, using the crib 'heil hitler', the pairings could be represented as such:

h:A
e:Z
i:N
l:C
h:Z
i:E
t:A
l:P
e:B
r:H

Source: Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

This will indicate which letter a particular cipher text letter represents. By writing down which letter matches up to which in the key and cipher alphabet, he can more easily see which possible disks could have been used on that particular letter. Through the use of a table, a cryptanalyst can create a way to visualize the possible orders of the disk and begin the real cipher work.

First, each letter pair should be listed at the top of the table. Similarly, all of the disks (Disk 1, Disk 2 etc.) are recorded in the far left column of the table. Then, in each space beneath a letter pair, how far apart the two letters are found on the corresponding disk is written down. This is done by counting from one letter to another in one direction and recording the found value. In each row of this table, the specific disks that are being examined are listed in order 1-10.

	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
1:	15									
2:	14									
3:	15									
4:	18									
5:	4									
6:	22									
7:	14									
8:	21									
9:	11									
10:	5									

Source: Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

After finding out how far apart each of the two letters are in the first disk, the cryptanalyst should proceed to find the distance on the nine remaining disks. Once this first column is filled out, they can continue to check the second lettering pair that was found. This same process is repeated until the entire cross-section of the table is filled in.

	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
1:	15	1	6	12	13	14	10	9	10	19
2:	14	5	6	3	16	4	22	23	25	7
3:	15	15	4	2	17	12	14	25	10	7
4:	18	7	10	7	14	20	12	25	1	6
5:	4	14	20	13	20	7	21	14	25	24
6:	22	16	3	17	10	19	1	14	14	14
7:	14	15	14	8	7	12	15	19	12	13
8:	21	12	12	22	5	2	14	8	8	14
9:	11	14	15	14	15	14	16	25	5	2
10:	5	23	5	21	17	21	20	6	14	12

Source: Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

After every letter pair has been evaluated on each disk, the cryptanalyst faces a ten by ten table filled with numbers representing the distance between the two letters used

in the pair. The next task for the code-breaker is to determine which order of disks works for the known crib and cipher.

	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
1:	–	–	–	–	–	14	–	–	–	–
2:	14	–	–	–	–	–	–	–	–	–
3:	–	–	–	–	–	–	14	–	–	–
4:	–	–	–	–	14	–	–	–	–	–
5:	–	14	–	–	–	–	–	14	–	–
6:	–	–	–	–	–	–	–	14	14	14
7:	14	–	14	–	–	–	–	–	–	–
8:	–	–	–	–	–	–	14	–	–	14
9:	–	14	–	14	–	14	–	–	–	–
10:	–	–	–	–	–	–	–	–	14	–

Source: Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

By looking for commonalities in each column, the most likely arrangement of cylinder disks can be determined. This technique works because the cipher text and the actual message will always be the same distance apart. Therefore, there will be at least one reoccurring number in every column. This number, once again, represents the distance between the letter pair. Once the number that occurs in every column is determined, the cryptanalyst must find an order that works for the message. It is important to note that there is a possibility that more than one number could appear in every column. The only way to alleviate this dilemma is by performing the following test on both numbers.

By arranging the disks so that each time you move over a column, or letter pair, the corresponding disk used has the correct distance between letters, you can find the orders of the disks. In the table, the numbers form a diagonal line across the table,

thereby making it easy to identify when the correct order, represented by the highlighted column, has been obtained.

	h:A	e:Z	i:N	l:C	h:Z	i:E	t:A	l:P	e:B	r:H
2:	14	–	–	–	–	–	–	–	–	–
5:	–	14	–	–	–	–	–	14	–	–
7:	14	–	14	–	–	–	–	–	–	–
9:	–	14	–	14	–	14	–	–	–	–
4:	–	–	–	–	14	–	–	–	–	–
1:	–	–	–	–	–	14	–	–	–	–
3:	–	–	–	–	–	–	14	–	–	–
6:	–	–	–	–	–	–	–	14	14	14
10:	–	–	–	–	–	–	–	–	14	–
8:	–	–	–	–	–	–	14	–	–	14

Source: Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

After this arrangement has been determined, the cryptanalyst working on the cylinder could move around his own cylinder's disks to the order that he found. With the disks in the right sequence, a code-interceptor could conceivably break any number of ciphers that they receive from this source, assuming the order of the cylinders does not change.

However, the chance that someone would intercept the cipher and plain text is very slim. Even more unlikely is the fact that in this case, our crib and the number of disks corresponded perfectly. With a shorter crib, more information would have been necessary in order to find out the arrangement of all of the cylinders. This is perhaps the reason why the cylinder was used for such an extensive amount of time. It is near impossible to decipher without given information. Additionally, it is easily enhanced through the addition of more disks. For instance, by increasing the number of disks to 11, the cylinder goes from 3,628,800 (10!) possibilities to 39,916,800 (11!) potential

arrangements. The sheer amount of possibilities increased by each cylinder is incentive enough to make Bazeries cylinders with more disks.

History shows the process of modification that Jefferson's initial idea underwent which resulted in something that was applicable in each day and age. Despite not being used until almost a century after its conception, it proved to be one of the most successful encrypting methods during this time period. The advancement of his premise led to the successful enciphering of codes that went unbroken by the Third Reich until the fifth year of World War II. It revolutionized the way cryptography, particularly American cryptography, worked in a time where it was far behind other methods. The Bazeries Cylinder also shows a shift towards the mechanization of cryptography. This shift manifests itself more obviously through some of the machines during World War II, in particular the Engima, but was nonetheless initiated with Jefferson's wheel cipher in the late eighteenth century.

Works Cited

Barr, Thomas H. Invitation to Cryptology. Upper Saddle River: Prentice Hall, 2002.

Bruff, Derek. Cryptography 115F. 1 November 2010 . 1 November 2010 <http://derekbruff.com/teaching/cryptotimeline.htm>.

Goebel, Greg. Greg Goebel / In the Public Domain. 1 November 2010. 27 October 2010 <http://www.vectorsite.net/ttcode_05.html#m2>.

Kahn, David. The Code Breakers. 1967.

Torrone, Phillip. "Happy President's Day from MAKE." 18 February 2008. MAKE. 30 October 2010 <http://blog.makezine.com/archive/2008/02/happy_presidents_day_from.html>.