Eric Roberts
CS 54N

Handout #19
October 31, 2016

Cryptography

Cryptography

Eric Roberts
CS 54N
October 31, 2016

Cryptograms

- A ***cryptogram*** is a puzzle in which a message is encoded by replacing each letter in the original text with some other letter. The substitution pattern remains the same throughout the message. Your job in solving a cryptogram is to figure out this correspondence.
- One of the most famous cryptograms was written by Edgar Allan Poe in his short story "The Gold Bug."
- In this story, Poe describes the technique of assuming that the most common letters in the coded message correspond to the most common letters in English, which are E, T, A, O, I, N, S, H, R, D, L, and U.

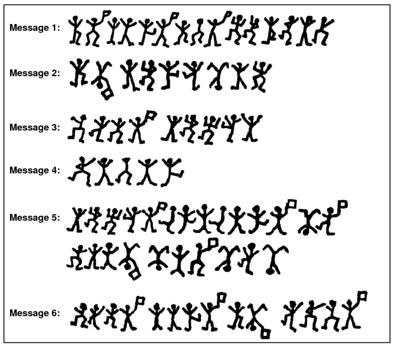
Edgar Allan Poe (1809-1849)

Poe's Cryptogram Puzzle

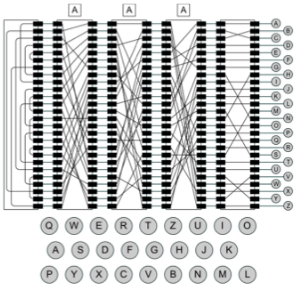
```
53‡‡†305))6*;4826)4‡•)4‡);806*;48†8¶
60))85;1‡(;:‡*8†83(88)5*†;46(;88*96*
?;8)*‡(;485);5*†2:*‡(;4956*2(5*–4)8¶
8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(
‡?34;48)4‡;161;:188;‡?;
```

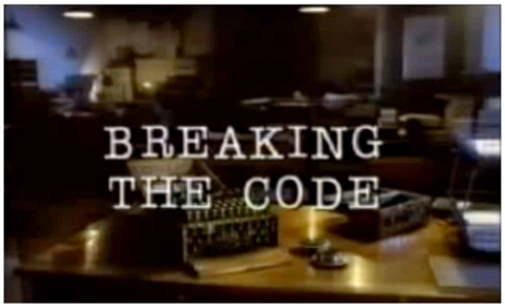
8	33
;	26
4	19
‡	16
)	16
*	13
5	12
6	11
(	10
†	8
1	8
0	6
9	5
2	5
:	4
3	4
?	3
¶	2
–	1
•	1

Sherlock Holmes's Dancing Men



The Enigma Machine





Important Properties of the Enigma Code

- The decryption team at Bletchley was able to exploit the following facts about the Enigma machine:
  - The encoding is symmetrical.
  - The Enigma machine can never map a character into itself.
  - The steckerboard does not affect the transformation pattern of the rotors, but only the characters to which the outputs of that rotor are assigned.
- The codebreakers were also helped by the fact that the Germans were often both careless and overconfident. In believing they had an unbreakable encoding machine, they failed to take adequate measures to safeguard the integrity of their communications.

Breaking the Enigma Code

- The most common technique used at Bletchley Park was the ***known-plaintext attack,*** in which the codebreakers guess that a particular sequence of characters exists somewhere in the decoded message. A sequence of characters that you guess is part of the plaintext is called a ***crib.***
- Breaking an Enigma message required the following steps:
  - Align the crib with the ciphertext to eliminate ***crashes*** in which a letter appears to map to itself.
  - Create a ***menu*** recording the links between letter pairs in the crib and ciphertext.
  - Identify ***loops*** in the menu at which a chain of letter pairs cycles back to the original letter.
  - Use the loops in the menu to create a wiring pattern for an electromechanical device called a ***Bombe*** that searches for settings of the Enigma rotors that produce the observed pattern.

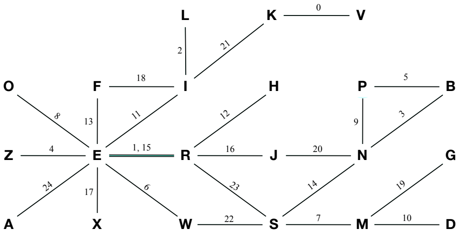
Step 1: Align the Crib and Ciphertext

U A E N F V R L B Z P W M E P M I H F S R J X F M J K W R A X Q E Z
K E I N E B E S O N D E R E N E R E I G N I S S E

No crashes exist in this alignment, so it is a feasible solution.

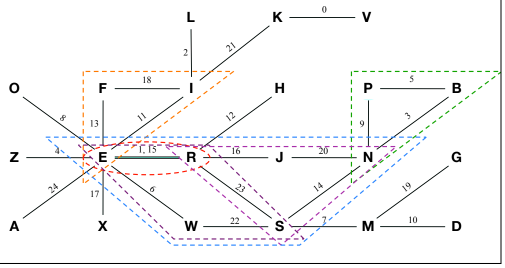
Step 2: Construct the Menu

V R L B Z P W M E P M I H F S R J X F M J K W R A
K E I N E B E S O N D E R E N E R E I G N I S S E
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24



Step 3: Find the Loops

V R L B Z P W M E P M I H F S R J X F M J K W R A
K E I N E B E S O N D E R E N E R E I G N I S S E
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24



Exercise: Enigma Decryption

On D-Day (June 6, 1944), the first Enigma decrypt used the following crib:

WETTERVORHERSAGEBISKAYA

You believe that this crib exists somewhere in the following ciphertext:

QFZWRWIVTYRESXBFOGKUHQBAISEZ

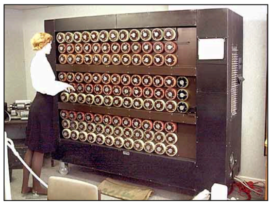
Create the menu that Alan Turing and his Bletchley Park colleagues would use to program the Bombe.

Cryptography—Bletchley Park

Bletchley
Oxford

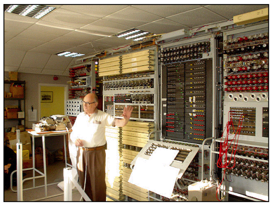
I've twice had the opportunity to teach this course in England, where it was possible to visit Bletchley Park—the home of the Government Code and Cipher School (GCCS), where the Enigma code was broken.

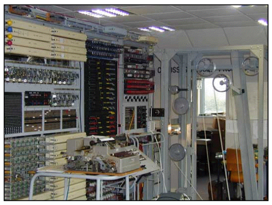
Cryptography—Bletchley Park



In our field trips to Bletchley Park, our tour was led by Jean Valentine, who worked with the Bombe decryption machine shown in these pictures.

The Colossus Machine





On our tour of Bletchley Park, my Oxford class also had a chance to see Tony Sale's reconstruction of Colossus, which broke the German diplomatic code. The Colossus machine was phenomenally fast for its day, reading 300 characters per second.