Eric Roberts and Jerry Cain
CS 106J

Handout #28
May 5, 2017

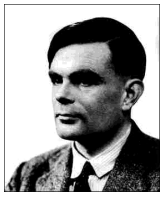
Cryptography

Cryptography

Eric Roberts and Jerry Cain
CS 106J
May 5, 2017

Alan Turing

- The film *The Imitation* Game celebrated the life of Alan Turing, who made many important contributions in many areas of computer science, including hardware design, computability, and AI.
- During World War II, Turing headed the mathematics division at Bletchley Park in England, which broke the German Enigma code—a process you'll simulate in Assignment #4.
- Tragically, Turing committed suicide in 1954 after being convicted on a charge of "gross indecency" for homosexual behavior. Prime Minister Gordon Brown issued a public apology in 2009.



Alan Turing (1912-1954)

The Imitation Game

- Alan Turing's wartime work is now more widely known because of the movie *The Imitation Game*.

- Unfortunately, the movie got much of the history wrong.

Encryption

Twas brillig, and the slithy toves,
Did gyre and gimble in the wabe:
All mimsy were the borogoves,
And the mome raths outgrabe.

Twas brillig, and the slithy toves,
Did gyre and gimble in the wabe:
All mimsy were the borogoves,
And the mome raths outgrabe.

Implementing a Caesar Cipher

```
caesarCipher("Et tu, Brute?", -13)
function caesarCipher(str, key) {
   if (key < 0) key = 26 - (-key % 26);
   var result = "";
   for ( var i = 0 ; i < str.length ; i++ ) {
      var ch = str.charAt(i);
      if (ch >= "A" && ch <= "Z") {
         var code = ch.charCodeAt(0);
         var base = "A".charCodeAt(0);
         ch = String.fromCharCode(base + (code - base + key) % 26);
      } else if (ch >= "a" && ch <= "z") {
         var code = ch.charCodeAt(0);
         var base = "a".charCodeAt(0);
         ch = String.fromCharCode(base + (code - base + key) % 26);
      }
      result += ch;
   }
   return result;
}
```

str	result	key	i	code	base	ch

Console

```
> caesarCipher("Et tu, Brute?", -13)
Rg gh, Oehgr?
```

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

```
AGOODGLASSINTHEBISHOPSHOSTELINTHEDEV
ILSSEATFORTYONEDEGREESANDTHIRTEENMIN
UTESNORTHEASTANDBYNORTHMAINBRANCHSEV
ENTHLIMBEASTSIDESHOOTFROMTHELEFTEYEO
FTHEDEATHSHEADABEELINEFROMTHETREETHR
OUGHTHESHOTFIFTYFEETOUT
```

Exercise: Letter-Substitution Cipher

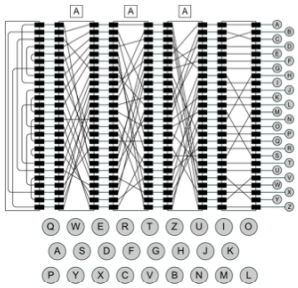
Poe's cryptogram is an example of a ***letter-substitution cipher,*** in which each letter in the original message is replaced by some different letter in the coded version of that message. In this type of cipher, the key is usually presented as a sequence of 26 letters that shows how each of the letters in the standard alphabet are mapped into their enciphered counterparts:

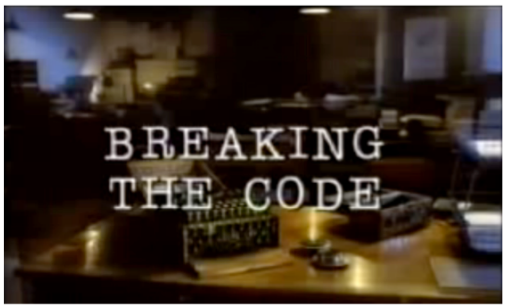
```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
```

JavaScript Console

```
> const KEY = "QWERTYUIOPASDFGHJKLZXCVBNM";
> encrypt("SECRET MESSAGE", KEY)
LTEKTZ DTLLQUT
```

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.***
- *The Imitation Game* gives the mistaken impression that Alan Turing came up with the idea of a crib during the war. The value of a crib has been known since antiquity.
- The 2001 movie *Enigma* offers a much more accurate view of why cribs are important and how codebreakers use them.