

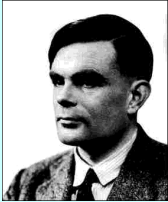
Cryptography

Jerry Cain
CS 106AJ
October 26, 2018
slides courtesy of Eric Roberts

Once upon a time . . .

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 #5.
- 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.

Cryptography

Encryption



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

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

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

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.

The End