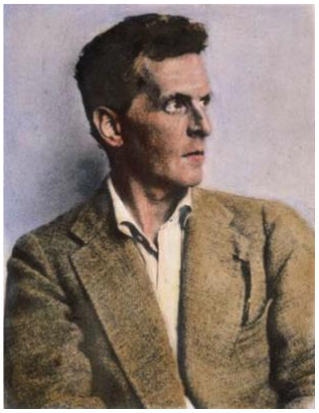
FYSE 1280 Fall 2025

Breaking The Code: The Enigma of Alan Turing

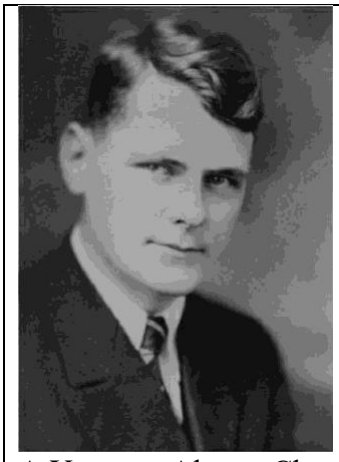
Assignment 8

For Wednesday, October 1



Ludwig Wittgenstein

Henryk Zygalski, Jerzy Rózycki, and Marian Rejewski
1941 in Cadix France



A Younger Alonzo Church

Faculty Lounge in Princeton's Fine Hall.

Reading

Read Chapter 5 "The Tender Peel" of David Leavitt, *The Man Who Knew Too Much: Alan Turing and the Invention of the Computer.*

Writing

Outline for Essay 2.

Writing: **The Ethics of Reading Other People's Mail**

Suggested Length: 4 -5 pages

Due Dates:

Wednesday, October 1: Outline
Wednesday, October 8: First Draft
Week of October 8: Conference with Maggie Wong
Friday, October 24: Final Draft

After the success American codebreakers had in World War I, the United States set up its first peace time cryptanalytic office. Officially designated MI-8 or the Cipher Bureau, it became known as the *American Black Chamber*. The Black Chamber was very successful during the 1920's in decrypting the diplomatic communications of many nations.

When newly appointed Secretary of State Henry Lewis Stimson learned of the Black Chamber, he shut down the operation in 1929, citing an ethical standard: "Gentlemen don't read each other's mail."

Ninety-five years later, we find the Black Chamber's descendent, the National Security Agency, regularly intercepting not only the communications of allied nations, potential foes and "terrorist" organizations, but also the telephone calls and emails of many of our own citizens. Corporations and colleges sometimes read the emails of their employees and students. Individuals routinely strip off the encryption from videos and audio recordings to make personal copies without paying for them. Hackers break into organizations' websites and databases with increasing frequency.

Most of these activities involve some form of codebreaking, removing a layer of security that was meant to limit access to the underlying message or data. Some of these actions may be ethical, others not. In this paper, we ask you first to relate your own personal experiences in this area. When you've had the opportunity (or temptation) to read an intercepted message or make an illegal copy, what did you do and how did you justify your action? Then you need to propose and defend an ethical standard for deciding when, if ever, it is justifiable to examine and use information that you weren't meant to see (or at least not entitled to see without paying for access). Describe some particular scenarios where you would consider it ethical to engage in such forms of codebreaking and some situations where it would be unethical. Should governments and corporations be required to adhere to the same standard as individuals?

In the wake of shootings on their campuses and the increase in suicides, it's been proposed that colleges regularly monitor their students' email in an effort to identify individuals whose messages indicate they might be likely to commit violence on themselves or others. Advocates assert that such action would save lives. Opponents say it is an unwarranted attack on privacy.

NOTES

There are three parts to the essay: (a) A personal experience with "codebreaking," broadly interpreted (roughly 1 page);

(b) A discussion of justifiable and unjustifiable forms of codebreaking, developing an ethical standard for when it is justified. (roughly 2 -3 pages), and

(c) A statement about how you would vote on a policy to allow Middlebury to routinely monitor student email and how you would justify your vote. (roughly 1 page)