


Background Data:
Naval Warfare, Battle of the Atlantic, Cryptography, and the Code Game

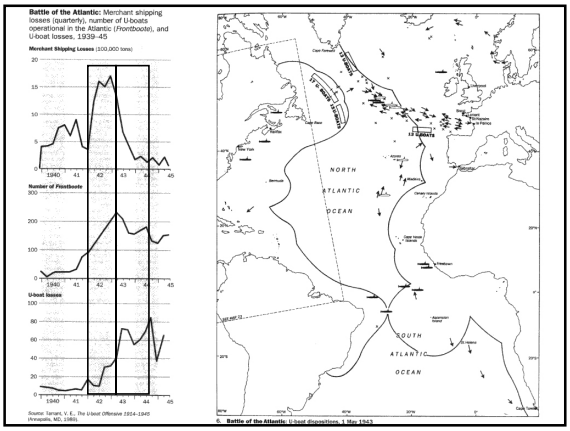
Randy H. Katz
CS Division, EECS Dept.
University of California, Berkeley
Spring 2005


Battle of the Atlantic
Allied Convoys vs. German U-Boats

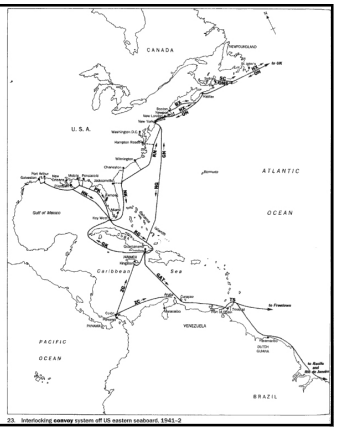
- Germans on the Offensive, Allies on the Defensive
  - Choosing Targets
  - Assembling Forces
  - Finding the Enemy
  - Attacking with Precision or Causing As Much Damage as Possible
  - Avoiding/Surviving Defenders
  - Determining the Effects of Naval Combat

Battle of the Atlantic
Allied Convoys vs. German U-Boats

- Allies on the Offensive, Germans on the Defensive
  - Choosing Targets
  - Assembling Forces
  - Finding the Enemy
  - Attacking with Precision or Causing As Much Damage as Possible
  - Avoiding/Surviving Defenders
  - Determining the Effects of Naval Combat

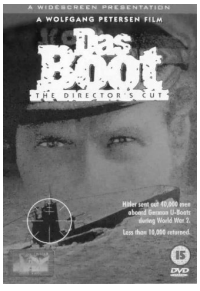


Convoys



"Das Boot"






Naval Intelligence
Finding the Enemy, Hiding Your Forces

- Is an "unbreakable" code possible?
- Is it possible to "hide" coded transmissions?
- How do you balance the need to communicate with the need to be invisible to easedropping?
- Cryptography, Cryptanalysis
  - Heroic Codebreaking: Enigma, the Battle of the Atlantic, and the Development of the Computer
  - Codebreaking in the Pacific: Intelligence successes at Midway
- Technology and the Battle of the Atlantic
  - Airborne Radars, High Frequency Direction Finding

Signals Intelligence

- Collecting information about a (potential) foe's capabilities (economic, military) and intentions (political, military) as old as nations themselves!
- New about the late 19th and 20th Centuries:
  - Rise of far-flung empires, increasing use of technologies for communications, need for command and control

Development of Communications Technology

- Commercial = Militarily Relevant Technologies
  - Electric Telegraph (1837)
  - Undersea Cables (1842); transatlantic cable (1866)
  - Transcontinental Telegraph (1861); crucial role in American Civil War
  - Marconi, Radio (1895): first customer--the Royal Navy!
- Counter measures: cut foe's undersea cables, message interception, message deception;
- Counter counter measure: radio communications
- Counter counter counter measure: jamming, direction finding
- Every measure has a counter measure, and in turn, a counter-counter measure!

To Communicate is to Reveal

- Communication methods lead to detection
  - Can the detector be detected? identified as to individual and location?
  - Can the interceptor be fooled? traffic analysis and deception?
  - Can the communicator be stopped from successfully communicating? jamming?
  - Can the communicator hide his/her communications? stealth?

Intelligence Collection

- Spying, reconnaissance, spy satellites, code breaking
- Human intelligence (HUMINT) aka spies
- Signal intelligence (SIGINT)/Communications intelligence (COMINT) often used interchangeable, especially up through WWII
  - Modern militaries use many forms of electromagnetic radiation that don't involve communications, but are used for detection (e.g., RADAR)
  - Information derived from the monitoring, interception, decryption and evaluation of enemy radio communications
  - Naval intelligence particularly important, as until the development of recon satellites, the ability to put "eyes" at sea was very limited!

Codebreaking

- Before the Age of Radio, much more difficult to intercept cable traffic
- Radio potentially places large numbers of encrypted messages in the hands of the cryptanalysts
  - Key to breaking the code!
  - British Admiralty Room 40: Codebreaking Room

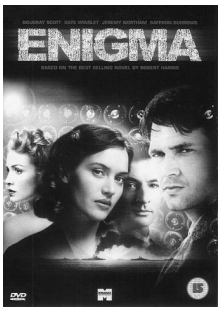
Enigma Machine

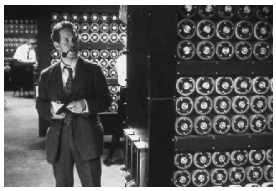
- Existence of ULTRA ("Very Special Intelligence") first revealed in 1974! Changed completely the way we view the history of WW II
- Combined encoding/decoding machine
  - Five rotor system, three in use at any time
  - How it worked and why it was hard to crack
    - Use of per message keys makes analysis difficult
    - But patterns provide the way in: doubly encrypted message keys
    - Poles reverse engineer a stolen Enigma machine
    - Invention of the Bombe: mechanical device to exhaust all enumerations
    - New Enigma stumps the Poles who turn to the British (1939)

Bletchley Park

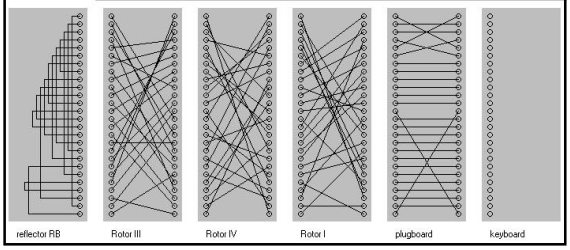
- Guessing the day key: cillies—common three letter sequences
- Human operator weakness!
- Rules of usage also limit the alternatives
- Stereotypical message structure helps too
- Turing's idea: the crib--<common plain text, encrypted text>
- If found, then could determine Enigma settings
- Compute the transformation in parallel: Turing's Bombe
- 10 May 40: Germans change their message key scheme
- Naval codes hardest to break—more sophisticated Enigma used
- Battle of Atlantic was being lost! Solution: pinch the codebooks!

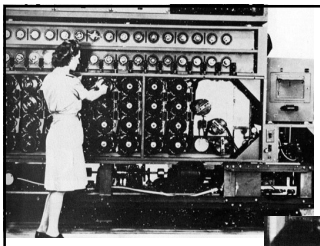
"Enigma"



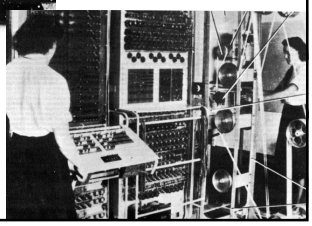


Enigma Deciphered





The Bombe



Colossus

The Code Game

% Letter Occurrence in English Text

a	7.49	n	6.74
b	1.29	o	7.37
c	3.54	p	2.43
d	3.62	q	0.26
e	14.00	r	6.14
f	2.18	s	6.95
g	1.74	t	9.85
h	4.22	u	3.00
i	6.65	v	1.16
j	0.27	w	1.69
k	0.47	x	0.28
l	3.57	y	1.64
m	3.39	z	0.04

The Code Game
More Text Analysis

- Common Digrams:
  - th he at st an in ea nd er en re nt to es on ed is ti
- Common Trigrams:
  - the and tha hat ent ion for tio has edt tis ers res ter con ing men tho
- Double Letters:
  - ll tt ss ee pp oo rr ff cc dd nn
- Common word ending letters:
  - e t s d n r y
- Most common words:
  - the of are I and you a can to he her that in was is has it him his

Next Week
Missiles and the Cuban Missile Crisis

- See class web page for readings:
  - Ballistic Missile Defense
    - http://www.missilethreat.com/overview/
  - Cuban Missile Crisis
    - http://www.gwu.edu/~nsarchiv/nsa/cuba_mis_cri/
  - 14 Days in October Web Site
    - http://library.thinkquest.org/11046/