

HNR 304 – 002
Spring 2008
Cryptology
Course requirements

Cryptography and cryptanalysis exercises (40%): Throughout the course you will be asked to encrypt messages using techniques of classical cryptography and you will be challenged to cryptanalyze messages encrypted by others in the class. You will be asked to discuss your success or failure attempting to cryptanalyze ciphertext messages.

Short paper (4 – 6 pages) about Alan Turing (20%): This paper is due on R, April 17. The paper should be submitted electronically as a .doc or .pdf file. This paper may be based upon a book about Turing or the play *Breaking the Code*, which will be performed by NKU Theater March 22, 25, 27, 29, April 2, 4, and 6. *Breaking the Code* is also available on video.

Here are three biographies about Turing:

Hodges, Andrew, *Alan Turing: The Enigma*, Vintage, 1992.

The definitive biography of Turing, one of the leaders at Bletchley Park. Quite long.

Leavitt, David, *The Man Who Knew Too Much: Alan Turing and the Invention of the Computer*, Atlas/Norton, 2006.

Not up to Hodges' standards, but shorter.

Turing, Sara, *Alan M. Turing*, Heffer, 1959.

A biography of Turing by his mother who writes surprising well.

Hodges' website <http://www.turing.org.uk/turing/> contains a great deal of material about Turing.

Medium length paper (7 – 10) based upon a book (20%): This paper is due on R, May 1. The paper should be submitted electronically as a .doc or .pdf file. You will write about the content of a book about cryptology. Some possible books are:

Early cryptology

Urban, Mark, *The Man Who Broke Napoleon's Codes*, Harper Collins, 2001.

About George Scovell, one of Wellington's officers, who fought cryptological battles with Napoleon's army 1809 – 1815.

Budiansky, Stephen, *Her Majesty's Spymaster: Elizabeth I, Sir Francis Walsingham and the Birth of Modern Espionage*, Viking, 2005.

Like the first chapter of Singh. More detail. Very thorough.

World War I and Between the World Wars

Friedman, William F., and Mendelsohn, Charles J., *The Zimmermann Telegram of January 16, 1917 and Its Cryptographic Background*, Aegean Press, 1994.

Originally classified; now declassified.

Kahn, David, *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*, Yale, 2004.

Fascinating character.

Pratt, Fletcher, *Secret and Urgent: The story of codes and ciphers*, Aegean Park Press, 1939.

Written between the wars. It would have been a good text for a cryptology course in 1939. It shows the state of cryptology just after Yardley.

Tuchman, Barbara W., *The Zimmerman Telegram*, Ballantine, 1994.

The cryptological event that led to the US entering WWI. Originally published in 1958, additional information has become public since then. See Friedman and Mendelsohn above.

Yardley, Herbert O., *The American Black Chamber*, Aegean Park Press, 1931.

A shock when it was first published. It reveals US codebreaking efforts during World War I and the naval conference that followed the war.

World War II

Bletchley Park and Bletchley Park People

Denniston, Robin, *Thirty Secret Years: A.G. Denniston's Work in Signals Intelligence 1914 – 1944*, Polperro Heritage Press, 2007.

Alastair Denniston developed the Bletchley Park team.

Hill, Marion, *Bletchley Park People*, Sutton, 2004.

It's about ... well, Bletchley Park people.

Hinsley, F.H., and Stripp, Alan (eds), *Codebreakers: The inside story of Bletchley Park*, Oxford, 1993.

Essays by some of the men and women who worked at Bletchley Park.

Smith, Michael, *Station X: Decoding Nazi Secrets*, TV Books, 1999.

Based upon the NOVA show of the same name. Station X = Bletchley Park.

Smith, Michael, and Erskine, Ralph, *Action this Day: Bletchley Park from the breaking of the Enigma Code to the birth of the modern computer*, Bantam, 2001.

Like Hinsley and Stripp – essays by people who were at Bletchley Park or who have studied what happened there.

Watkins, Gwen, *Cracking the Luftwaffe Codes*, Greenhill Books, 2006.

The author was a codebreaker at Bletchley Park.

Welchman, Gordon, *The Hut Six Story*, Baldwin, Cleobury Mortimer, 1997.

Another story of Bletchley Park by one of the major players.

Winterbotham, F.W., *The Ultra Secret*, Harper and Row, 1974.

The book that broke the Bletchley Park secret.

Enigma

DeBrosse, Jim, and Burke, Colin, *The Secret in Building 26: The Untold Story of America's Ultra War Against the U-Boat Enigma Codes*, Random House, 2004.

Local interest. Building 26 is in the NCR complex in Dayton, OH. This is the story of building the American bombe. (Also a DVD)

Kahn, David, *Seizing the Enigma: The race to break the German U-boat codes*, Barnes and Noble, 1998.

An "update" of Kahn's *The Code Book* with "new" material about the U-boat war in the Atlantic. The real U-571 story.

Kozaczuk, Wladyslaw, *Enigma: How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two*, University Publications of America, 1984.

The story of the Polish attacks on Enigma just prior to World War II.

Kozaczuk, Wladyslaw and Straszak, Jerzy, *Enigma: How the Poles Broke the Nazi Code*, Hippocrene Books, 2004.

A brief version of the previous book.

Sebag-Montefiore, Hugh, *Enigma: The battle for the code*, Wiley, 2000.

A detailed history of the battle to break Enigma.

Codemakers/Codebreakers

Marks, Leo, *Between Silk and Cyanide: A Codemaker's War 1941 – 1945*, Free Press, 1998.

A (very British) view of codemaking.

Rowlett, Frank B., *The Story of Magic: Memoirs of an American Cryptologic Pioneer*, Aegean Park Press, 1998.

The story of the cryptologic war against Japan by the cryptologist in charge of the U.S. Army group responsible for breaking Japanese diplomatic codes and ciphers, including the PURPLE machine.

Pacific Theater

Smith, Michael, *The Emperor's Codes: The Breaking of Japan's Secret Ciphers*, Arcade, 2000.

The United States' battle with Japanese codes and ciphers.

Stripp, Alan, *Codebreaker in the Far East*, Oxford, 1989.

About Bletchley Park's work in the Far East. By one of the participants.

Comprehensive World War II History of Cryptology

Budiansky, Stephen, *Battle of Wits: The Complete Story of Codebreaking in World War II*, Free Press, 2000.

The title describes it. Very well done.

Fiction

Harris, Robert, *Enigma*, Random House, 1995.

A fictionalized account of the work at Bletchley Park. (Also a movie)

Stephenson, Neal, *Cryptonomicon*, Avon Books, 1999.

A ([really] long) novel that leaps back and forth between World War II and today. A lot has been written about this book, its characters, what's true, what's not, etc.

NSA

Bamford, James, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, Penguin Books, 1983 (< Houghton Mifflin Company, 1982).

The bestseller about the history of the NSA. The first book to reveal that NSA exists. Lots of detail about organization and NSA's early history. Controversial.

Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century*, Doubleday, 2001.

An update of *The Puzzle Palace*. Events that are of more interest to the present-day reader.

Brown, Dan, *Digital Fortress*, various publishers.

Fiction!!!! The author of *The Da Vinci Code* takes on the NSA and loses. This is a really bogus plot. Nothing like reality (just like *The Da Vinci Code*).

Burrows, William E., *By Any Means Necessary: America's Secret Air War in the Cold War*, Farrar, Straus, and Giroux, 2001.

About the aircrews who captured Communist bloc signals.

Sontag, Sherry, and Drew, Christopher, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, Public Affairs, 1998.

Also, summarized in an History Channel Video.

Privacy

Keffe, Patrick Radden, *Chatter: Dispatches from the Secret World of Global Eavesdropping*, Random House, 2005.

UKUSA, Echelon, and more.

Levy, Steven, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*, Viking, 2001.

Not great literature, but a look at the development of public key cryptology. The author's bias is evident in the title.

Cryptological History

Kahn, David, *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet*, Scribner, 1967.

The definitive history of cryptology. But Cryptology is often secret stuff; so, from World War II on, this book is not definitive.

You may chose a chapter of this book.

Project and presentation (20%): The presentations will be made during the last 4 class days. You will have 20 minutes for a presentation – 15 minutes for the presentation and 5 minutes for questions. Two people may work together on a project. Topics will be suggested; however, you are not restricted to those. Please discuss your preliminary topic with me prior to spring break. You may modify your ideas as you proceed with the project.

A Few Project Ideas:

Alan Turing and the portrayal of him in the play *Breaking the Code* compared to the “Turing character” in *Enigma*.

The impact of cryptology on an historical event.

Examples of cryptology in literature.

Contrast life at Bletchley Park with the portrayal in the film (and book) *Enigma*.

The Navajo Codetalkers of World War II and their portrayal in *Windtalkers*.

Attempts to steal the Enigma machine and a portrayal in *U-571*.

The contribution of NCR of Dayton to the breaking of the Enigma messages, which is described in *Building 26*.

Cryptological machines of World War II.

Examine how the NSA is portrayed in films and books (e.g., the film *Enemy of the State* and the book *Digital Fortress*).

A current issue in cryptography; e.g., the impact of cryptology on civil liberties, on securing internet commerce, or on law enforcement.

Write an encryption or decryption or cryptanalysis program.

Explore the Hill cipher (requires some linear algebra).

How did Jules Verne learn his cryptology? From Poe?

Is your car safe? Can Keyloq be broken?

Did Roosevelt know about the Pearl Harbor attack before it happened?

Why cryptologists worried about quantum computers?

What's quantum key exchange?

William and Elizibeth Friedman.

The three Polish mathematicians who broke Enigma prior to World War II.

Recruiting codebreakers -- today vs. World War II.