

Dr. Linda Sundbye
MTH 4390, 4590 - Senior Seminar
Introduction to Cryptology
Fall 2009

A List of Possible Projects

1. Ancient Languages

Egyptian Hieroglyphics, Rosetta Stone
Decipherment of Linear B - An ancient script used in ancient Greece circa 1500 BC; Linear A
Cuneiform - Form of writing used in ancient Babylon
Mayan hieroglyphics
The I Ching

2. Cryptology in Literature

“The DaVinci Code” by Dan Brown
“The Gold Bug” by Edgar Allen Poe
“The Adventure of the Dancing Men” by Sherlock Holmes
“Cryptonomicon” by Neal Stephenson
“La Disparition” by Georges Perec, English translation by G. Adair

3. Episodes of Cryptology

The Beale Treasure
Bible Codes
The Cipher Challenge - Simon Singh

4. Classical Ciphers

Playfair cipher, used as a field cipher by the British in the Boer War and in World War I
Great Cipher of Louis XIV
Vigènere cipher

5. Wartime/Political Cryptology

Mary, Queen of Scots; Queen Elizabeth; Sir Francis Walsingham

World War I, Zimmerman telegram
World War II, Alan Turing, Marian Rejewski, Enigma, Ultra
World War II, Navajo Code Talkers
The Morse Code

6. Modern Cryptosystems and Issues

RSA Data security
The story of Pretty Good Privacy (PGP), Philip Zimmerman
Data Encryption Standard (DES)
Successor to Des - Advanced Encryption Standard (AES), Rijndael
Quantum Cryptography
The Clipper Chip
Problems of Key Escrow
Smart cards for debit, credit or identification
Security and the Internet, secure shells, virtually private networks
Blowfish
Elliptic Curve Cryptography
Sarah Flannery, Cayley-Purser algorithm; Flannery & Flannery, *In Code: A Young Women's Mathematical Journey* (2001).

7. Error Correcting Codes

8. Signals and codes used in sports such as baseball
9. Women in cryptology, women spies