Cryptology Instructor Notes

Introduction

- Codes are as old as civilization itself…as old as the need to keep secrets or to communicate.
- There are two parts to cryptology: making codes (Crytography) & breaking codes (Cryptanalysis).
- Examples of everyday codes:

Language (verbal/nonverbal)	binary code (computer language)
zip codes	bar codes
traffic lights/signs	plug wiring
fashion codes (groups, clicks, etc.)	cable/satellite scrambling
archeology	airplane flaggers

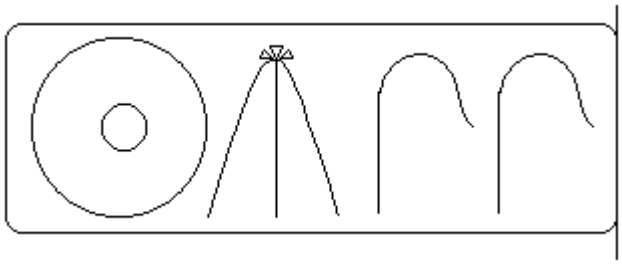
Definitions

- *Cryptography:* study of making codes
- *Cryptanalysis:* study of breaking codes
- *Cryptology:* study of both cryptography and cryptanalysis
- *Cipher:* procedure to render messages unintelligible except to the authorize recipient.
- *Encryption:* process of using the cipher to render messages unintelligible except to the authorized recipient.
- *Decryption:* process of recovering the original message from the obscured version.
- *Plaintext:* original, unencrypted message.
- *Ciphertext:* obscured, encrypted message.

- *Key:* secret shared between the sender and receiver.
- *Attack:* an attempt to decrypt encrypted messages without knowledge of the key.

Historical Ciphers

- *Words in wedges:* Mesopotamian scribes used a reed stylus to scratch pictograms into wet clay.
- *Riddle of glyphs:* Mayan people also used pictograms. Discuss Mayan numbers and Mayan zero. Aztecs also used pictures. A shield and a club represented war. A burning temple represented victory.
- *Unlocking the past:* One sophisticated 4000 year-old script from northern India has more than 400 different signs, and experts still have no idea what they mean.
- *Hieroglyph mystery:* Egyptian hieroglyphics were a mystery for years. In the 18th Century, Europeans visiting Egypt discovered remains, including puzzling picture writing, of a long since vanished civilization. No one was able to interpret the writing. In 1799, the French army occupied Egypt. Troops in Rosetta uncovered a large black slab weighing three-quarters of a ton. It had three sets of writing. The first was in hieroglyphs. The second was in a strange script called demotic, used by ancient Egyptians for everyday business and as a quick shorthand. The third was in ancient Greek, which scholars were quickly able to read. Still the hieroglyphs remained a mystery until 1814 when Thomas Young took a copy of the Rosetta stone with him on vacation. He discovered a series of characters in the hieroglyphs that he guessed must represent the name of Ptolemy. The ancient code was finally cracked completely by a Frenchman, Jean-Francois Champollion. In 1822 he found some hieroglyphs on the wall of the Abu Simbel temple in Egypt.



He discovered that the round disc stood for the coptic word RA and that the last two hieroglyphs both stood for the letter S. (RA – S S). He assumed correctly that the missing letter was an M (RA M S S). He also guessed that the scribes left out the vowels. So the hieroglyphs must stand for the name Rameses.

- *Secret Stick:* The Spartans were a very war-like city also fighting with its neighbors. For this reason they were often sending messages back and forth. So to make these messages undecipherable for their enemies they invented a secret code using a multisided stick called a scytale and a long strip of leather. This system made it possible for Sparta to win many battles.

- *Caesar Shift:* The Roman dictator Julius Caesar used secret writing a lot too. He is famous for what is now known as the Caesar shift. This is a substitution cipher where each letter in the alphabet is encrypted by shifting it three letters down in the alphabet. So *a* encrypts to *D*, *b* encrypts to *E*, and so on. Still if anyone intercepted a message and suspected that a shift cipher was used, they could easily go through the 26 possible shifts and decode the message.

- *Plotting & Scheming:* Mary (Roman Catholic), Queen of Scots, was queen of Scotland when one week old. In 1568 she fell out of favor with the Scottish nobles and was forced to flee. She went to her cousin Elizabeth I, Queen of England. Queen Elizabeth (a protestant) felt threatened by Mary and had her imprisoned. Mary was bitter with her cousin and plotted to have her killed and usurp the throne of England. She sent secret messages to her one of her strong supporters, Anthony Babington. She did not know however that her messages were being intercepted by one of Elizabeth's spies, Thomas Phelippes who was an expert code breaker. He quickly broke the code using frequency analysis. In one of the messages, Thomas added a line in an exact forgery of Mary's handwriting and asked Anthony to name all of the plotters. They were all arrested and killed. Mary was beheaded in 1587.

- *Square cipher:* Blaise Viginiere created a cipher that coded each letter in a message using a different shift. He made the Viginiere square and used a word or phrase as the key which determined which shift to use.

- *World War II:* During WWII, the US started out using a code that was painstakingly long and tedious the code and to decode. Each letter of a message was typed into the SIGABA cipher machine, and then the encrypted letters were noted on a piece of paper. Then the encrypted messages had to be sent via radio. The receiving end had to go through a similar process to decode the message. It took too much time and too much space for the equipment. Philip Johnson came up with the ingenius idea to use the Navajo language as the code. 29 Navajos were quickly trained and sent to the field. Navajo was unfamiliar to everyone outside the reservation which made it extremely secure. Lots of special code words had to be created to the things that the Navajos were not familiar with. Plane was a hummingbird, bombs were eggs, etc. This was one of the only codes in history that was never cracked.

  The Germans used a machine called the Enigma to encode their secret messages. It was a very complex and almost unbreakable cipher. More details later.

- *Beale Cipher:* Thomas Beale left three letters in a box that were encoded. This was in Buford, Virginia. Robert Morriss was left the key to the box. Morriss discovered that one of the letters was ciphered using the Declaration of Independence was the key to the second ciphered letter. He learned the treasure was buried 6 feet deep in a location about four miles from Buford. No one has ever cracked the ciphers used for the other two letters.

- *Zimmerman telegram:* Germans urged Mexico to attack US in order to prevent them from getting involved in the WWII. It was intercepted and cracked, unbenouced to the Germans.

- *Genetic code:* DNA

- *Morse code:* Letters are represented with a series of dots and dashes. Examples: – – – ... – – – (SOS)

Code Security & Usability

- What makes a code secure?

- *Key:*
  *How is the key sent from Alice to Bob?
  *What information does the key give if intercepted?
- *Encryption Process:*
  *How long does it take to encrypt a message?
  *How is the encrypted message sent from Alice to Bob?
  *What is done with hard copies of encrypted messages?
- *Decryption Process:*
  *How long does it take to decrypt a message?
  *What is done with <u>hard copies of decrypted messages?</u>

- How can you make an insecure code more secure?
  - *Remove spaces*
  - *Code stacking:* combine more than one cipher system in the encryption process.
- What factors determine a code's usability?
  - Time to encrypt.
  - Time to decrypt
  - Key length
  - Method for getting coded message and key from Alice to Bob.

Code Breaking Attacks

- *Ciphertext Only:* The cryptanalist possesses a fragment of the encrypted message but has no knowledge of the plaintext or of the key.
- *Frequency Analysis:* Analyze frequency of occurrence of characters, character combinations, and words.
  - Most common English characters: e, o, t.
  - Most common words: the, to, of, I, a.
  - Most common digrams: th, in, he, er
  - Most common trigrams: the, ing, and
- *Word Breaks:* When word breaks are known, look for one letter, two letter, and three letter words to get a good start to your cryptanalysis.
- *Known Plaintext:* The cryptanalist possesses all or part of a plaintext and corresponding ciphertext. The goal would be to deduce the key.
- *Crib:* A word or phrase which is known to occur somewhere in a plaintext message.