Crack the Code!

Dr. Heather Coughlin
California State University, Stanislaus

The Beginning: Steganography

Definition. Steganography is communicating through hiding the message.
steganos: 'covered'
graphein: 'to write'

Ancient Egypt: Rumored

Ancient Greece[2]:

- Hide messages under wax on wooden writing tablets. Greece was able to thwart surprise attack from Persia (480 BC).
- Shave head of messenger, write message on head, wait for hair to grow, send the messenger.
  Used to encourage a revolt against a Persian king.
- Pliny the Elder explained how to make invisible ink (1st Century AD).

Ancient China[2]:

- Write message on fine silk, roll into a tight ball, cover with wax, swallow.

15th Century, Italy[2]:

- Giovanni Porta developed ink which would sink through the shell of a hard-boiled egg, leaving the message on the egg.

Victorian England[2]:

- People would send "love letters" by pricking holes above letters in a newspaper. Sending newspapers was free, sending letters was expensive.

WWII:

- German spies in Central America used **microdots**. A microdot is a message that is shrunk to a dot, 1mm in diameter, and hidden in the punctuation of a letter.

The Next Step: Cryptography

Definitions

Cryptography: the art of creating and using methods to disguise messages

Cryptanalysis: the art of uncovering and recovering a disguised message

Cryptology: the study of cryptography and cryptanalysis

Code: substitution at the word/phrase level

Cipher: substitution at the letter level

Encode: scramble a message using a code

Decode: unscramble an encoded message

Encipher: scramble a message using a cipher

Decipher: unscramble an enciphered message

Encrypt: scramble a message using a code/cipher

Decrypt: unscramble an encoded/enciphered message

Cipher System: method for encrypting a message

Key: piece of information crucial for encryption/ decryption

Simple Substitution Ciphers

Substitute each letter according to a set rule.

Definitions:

Plain alphabet: abcdefghijklmnopqrstuvwxyz

Cipher alphabet: the alphabet after the plain alphabet has changed according to the cipher system

Plaintext: the original message
(convention: write in lower-case letters)

Ciphertext: the enciphered message
(convention: write in capital letters)

Example:

plaintext:	m	a	t	h	e	m	a	t	i	c	s
ciphertext:	J	N	E	L	A	J	N	E	Q	X	Y

The Caesar Cipher

Used in the Gallic Wars: 58 - 51 BC.

Take the plain alphabet and "shift it three places" (left).

plain alphabet:	a	b	c	d	e	f	g	h	i	j	k	l	m
cipher alphabet:	D	E	F	G	H	I	J	K	L	M	N	O	P

plain alphabet:	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher alphabet:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Example:

plaintext:	v	e	n	i,		v	i	d	i,		v	i	c	i
ciphertext:	Y	H	Q	L,		Y	L	G	L,		Y	L	F	L

Example: Make your own.

Shift Ciphers

The Caesar Cipher is an example of a shift cipher of three places.

Shift Cipher: a cipher using any "shift" of the plain alphabet.

Urban Legend: Decipher HAL (the computer from the movie *2001: A Space Odyssey*) using a shift cipher of one place.

Answer: ibm

Question: How do you decipher a message enciphered by a shift cipher?

Answer: Since the message was encrypted by a shift to the 'left' n places, shift the cipher alphabet to the 'right' n places.

Other Monoalphabetic Substitution Ciphers

Monoalphabetic Cipher: a cipher in which a single alphabet substitution is used.
Notes:

(1) There are $26! = 26 \times 25 \times 24 \times \cdots \times 3 \times 2 \times 1$ possible substitution ciphers.

(2) That is 403,291,461,126,605,635,584,000,000 possible substitution ciphers.

(3) To solve using "brute force" it would take a computer up to several hundred million years to crack a simple substitution cipher.

Keyword Cipher Alphabet:

(1) Pick a keyword, such as MATHEMATICS.

(2) Remove all repeated letters, i.e. MATHEICS.

(3) Build cipher alphabet by placing the fixed keyword first and then the rest of the alphabet, i.e.:

plain alphabet:	a	b	c	d	e	f	g	h	i	j	k	l	m
cipher alphabet:	M	A	T	H	E	I	C	S	B	D	F	G	J

plain alphabet:	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher alphabet:	K	L	N	O	P	Q	R	U	V	W	X	Y	Z

Improvements and Notes

(1) 1400's Europe: Heads of state use encryption

(2) Official cipher offices created.

(3) Used "nulls" for spaces

(4) used numbers 1 through 99 to represent letters (so 73 letters meant nothing.

(5) Codewords developed, codebooks developed.

(6) 1586: Mary Queen of Scotts is executed for treason. Plotting to kill Queen Elizabeth.
Sir Francis Walsingham (Queen's principal secretary) hired Thomas Phelippes to crack Mary's enciphered letters to coconspirators.

Transposition Ciphers

In a **transposition cipher**, only the original letters of the message are used. The letters will be rearranged in a particular fashion.

Spartan Scytale: (5th Century BC) Wrap a thin strip of paper around a staff. Write your message across the paper on the staff. Unwrap the paper to produce the enciphered message.

Railfence Transposition[2]: "The message is written with alternate letters on separate upper and lower lines." Then "smush" the letters together to form the ciphertext.

Example: plaintext: meet at noon

m e a n o
e t t o n

ciphertext: MEANOETTON

Solving Simple Substitution Ciphers

(1) Can you guess the context/content of the message?

(2) Use **Frequency Analysis**.

Notes:

(1) Cryptanalysis formally began in later part of the first millennium AD in the Middle East.

(2) Frequency analysis is the study of the frequency of occurrence of letters. (statistics)

(3) First treatise on frequency analysis was written by AbūYūsūf Ya'qūb ibn Is-hāq ibn as-Sabbāh ibn 'omrān ibn Ismaīl al-Kindī, the "philosopher of the Arabs."

Facts: (all about the English language)

(1) most common letters: E, T, N, O, R, I, A, S.

(2) more than half of all words end in E, T, D, S.

(3) Q is always followed by U.

(4) most common word: "THE."

(5) most common doublets: EE, TT, OO, SS, LL, FF.

(6) most common 2-letter combos: HE, RE, AN, TH, ER, IN.

(7) most common 3-letter combos: ION, AND, ING, THE, ENT.

Polyalphabetic Ciphers

Leon Battista Alberti: (1400's) Creates cipher disk. Is first to suggest using 2 or more cipher alphabets to encrypt a message.

Blaise de Vigènere: (1523) Creates the Vigènere cipher.

(1) Pick a **keyword**: special word agreed upon by sender and receiver. Example: ROOM

(2) Remove all repeated letters. Example: ROM

(3) Assign each letter of the alphabet a number: a=1, b=2, . . . , z=26.

(4) Write the modified keyword above your message:

keyword: R O M R O M R O

plaintext: i c e c r e a m

(5) Using the keyword, ROM=18, 15, 13, use the corresponding cipher alphabet from the Vigènere table to encipher the message.
Example: ARRUGRSB

Notes:

(1) The same cipher letter can represent different plain letter.

(2) The same plain letter may be represented by different cipher letters.

(3) Frequency analysis does not work on Vigènere cipher.

(4) Thought to be too slow and cumbersome for warfare, the Vigènere cipher was unused almost 200 years.

Black Chambers: (18th Century) Government cryptanalyst centers

Other Polyalphabetic Ciphers

Homophonic Substitution: Cipher system in which each letters is replaced by a variety of numbers (usually 01 – 99). The number of substitutes is proportional to the frequency of the letter.

The Great Cipher of Louis XIV: (1626) Created by Antoine and Bonaventure Rossignol.
Decrypted in the 1890's by Étienne Brazeries.
Pairs of numbers represented syllables.

Thomas Jefferson: (18th Century) Credited with inventing the cipher wheel.

36 wooden, independently moving, wheels mounted on an iron rod.
Each wheel marked with a different scrambled alphabet.
Set wheels so message reads across a horizontal line.
Use different horizontal line to encrypt message.
Receiver must have same wheels settings to decrypt the message.

Playfair Cipher

Sir Charles Wheatstone: (1854) Created a cipher he named after a friend, Lyon Playfair.

Used by the British through WWI.

Used as a backup cipher in WWII by the British and the Americans.

Algorithm and Example[7]:

(1) Pick a keyword. Example: MATHEMATICS[5]

(2) Write the keyword, without repetitions in a 5×5 square, combining I and J in one cell. Fill in the other letters in alphabetical order.

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

(3) Write your message with an "X" between any repeated letters. Break into pairs and use an "X" if needed at the end

Example: the moon is blue → th em ox on is bl ue

(4) If the letters of a pair lie on the same row: replace each letter by the letter to its immediate right, wrap around in same row if needed.

(5) If the letters of a pair lie on the same column: replace each letter by the letter directly below it, wrap up in same column if needed.

(6) If the letters of a pair lie in different rows and columns: locate the letters on the square and form a square. The letters of the opposite corners form the ciphertext. Cipher letter comes from the row of the plaintext letter.

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

M	A	T	H	E
I	C	S	B	D
F	G	K	L	N
O	P	Q	R	U
V	W	X	Y	Z

Ciphertext: HEMAQVUFCBLRZD

(7) To decrypt, go in opposite directions on the Playfair square.

Kerckhoff's Principle[2]: "The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key."

References

[1] National Security Agencey Kids Page, *http://www.nsa.gov/kids/home.cfm*, NOTE: this page has directions for making a Spartan Scytale and Cipher Wheel.

[2] Simon Singh, *The Code Book; The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, 1999.

[3] Robert Churchhouse, *Codes and Ciphers; Julius Caesar, the Enigma, and the Internet*, Cambridge University Press, 2002.

[4] H.X.Mel and Doris Baker, *Cryptography Decrypted*, Addison Wesley, 2001.

[5] Steven Roman, *Cryptology, Third Edition*, Modules in Mathematics, Innovative Textbooks, 1999.

[6] Cryptography FAQ, *http://www.faqs.org/faqs/cryptography-faq*

[7] Nova Online, Nazi Secrets, The Playfair Cipher, *http://www.pbs.org*