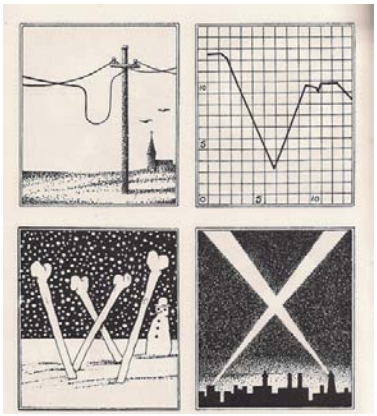
HANDOUT: WHAT IS CRYPTOGRAPHY?

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text

How do you think this message was encrypted?



Seven Secret Alphabets by Anthony Earnshaw

Can you solve this encryption?

20-15-4-1-25 25-15-21 23-9-12-12

12-5-1-18-14 1-2-15-21-20 3-15-4-5-19

What type of algorithm is this?

Types of Encryption

- *Substitution*
  - Replacing each letter with a different letter or symbol (a=@, b=J, c=2 so that "a cat" = "@ 2@J")
- *Transposition*
  - Rearranging the order of letters of the words of a message. (example: "the letters in each word get moved around = eth ttseelr ni ceah drow etg veodm uarndo")
- *Steganography*
  - Hiding a message (example: invisible inks, Herodotus tattooed messages on a shaved slave's head and waited for the hair to re-grow to hide his messages)
- *Mathematical*
  - Uses advanced formulas to encrypt text
- *Computer or Mechanically Assisted*
  - Using complex algorithms and any single or combination of the mathematical, transposition, substitution and steganography to encrypt plain text.

HANDOUT: FREQUENCY CHART

Letter	Relative frequency in the English language
a	8.167%
b	1.492%
c	2.782%
d	4.253%
e	12.702%
f	2.228%
g	2.015%
h	6.094%
i	6.966%
j	0.153%
k	0.772%
l	4.025%
m	2.406%
n	6.749%
o	7.507%
p	1.929%
q	0.095%
r	5.987%
s	6.327%
t	9.056%
u	2.758%
v	0.978%
w	2.360%
x	0.150%
y	1.974%
z	0.074%

Letter	Relative frequency as the first letter of an English word
a	11.602%
b	4.702%
c	3.511%
d	2.670%
e	2.007%
f	3.779%
g	1.950%
h	7.232%
i	6.286%
j	0.597%
k	0.590%
l	2.705%
m	4.374%
n	2.365%
o	6.264%
p	2.545%
q	0.173%
r	1.653%
s	7.755%
t	16.671%
u	1.487%
v	0.649%
w	6.753%
x	0.037%
y	1.620%
z	0.034%

Thinking about Letters....

Which letters do we use most frequently in English?

Which letters do we use less frequently?

How could you use this information to decrypt cipher text?

Want to know more about the frequency of letters?

Go to the Wikipedia: Letter Frequency page! You can learn which letters occur most frequently at the start of English words. And the frequency of letters in other languages! http://en.wikipedia.org/wiki/Letter_frequency

HANDOUT: YOU ARE THE CRYPTANALYST! ENCRYPT A MESSAGE!

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

Secret Message:

_____

_____

_____

HANDOUT: METHODS OF CRYPTOGRAPHY

Transposition

Rearranging the order of letters of the words of a message. (example: "the letters in each word get moved around = the elttres ni aehc owdr egt omevd rauodn").

Substitution

Replacing each letter with a different letter or symbol (a=@, b=J, c=2 so that "a cat" = "@ 2J@").

Introduction to Cryptanalyst Job

A kid produced video uses a hamburger analogy to describe the education necessary to become a cryptologist and jobs they can do. [elem 1.48 min]

http://www.youtube.com/watch?v=Q70kCNEFNRU&feature=related

Code Makers & Code Breakers

Excellent History Channel Modern Marvels YouTube Video [middle/high 15 mins]

http://www.youtube.com/watch?v=_H-jkS4KPAU

Mechanical Encryption Video

The most famous mechanical encryption device ever created was the Enigma machine. This video shows a real enigma machine and demonstrates why it was so effective.

http://www.youtube.com/watch?v=elYw4Ve4F-I

Steganography

Hiding messages (example: invisible inks, hiding text in pictures). Herodotus tattooed a message on a shaved slave's head and waited for the hair to regrow to hide his messages.

Mathematical

Uses advanced formulas to encrypt text

Computer assisted

Using complex algorithms and any single or combination of the mathematical, transposition, substitution and steganography to encrypt plain text.

Are the letters on the keyboard in order? Letter frequencies had a strong influence on the design of keyboard layouts. Why are they arranged the way they are?

TO SHARE WITH YOUR PARENTS

Cryptologists/Cryptanalyst

***Cryptologists**, communicate through secret writing such as codes, ciphers or a combination of both to keep messages safe from others. While cryptographers create, **cryptanalysts**, also known as code breakers, attempt to make decryption algorithms to read the secret codes. Cryptanalysts decipher secret coding systems and decode messages for the military, political, and law enforcement agencies and other organizations. Cryptologists develop encryption to help provide privacy for people and corporations, and keep hackers out of important data systems.*

EDUCATION

Most cryptanalysts have at least a bachelor's degree in math or computer science. They usually continue to take additional courses and training. In many cases an employer will provide and cover the cost of this training for qualified candidates. Additional pathways include foreign languages, criminology, information assurance and psychology.

WHERE THEY WORK

Cryptanalysts are employed by educational institutions, bank and trust companies, financial institutions, insurance companies, scientific institutions, and research agencies. They also may work for telecommunications companies, computer design firms, consulting firms, science and engineering firms, and all levels of government, including special services and intelligence agencies.

WHAT'S THE SALARY?

Low-end Salary: $63,930/yr
Median Salary: $101,645/yr
High-end Salary: $137,780/yr

WHAT COURSES DO I TAKE?

Math Math Math
- College Algebra
- Trigonometry
- Calculus I, II, III
- Linear Algebra
- Differential Equations
- Number Theory

Computer Science
Engineering
Foreign Languages
Criminology

FUN FACTOIDS

Cryptography scores highly on the WorkYourWay Index because it is a growing field with lots of new jobs, particularly in the field of information security and in government defense, the military and Homeland Security. Jobs in this field scored high for their above average salaries and the opportunity to give back to society (protect fellow citizens, protect your country, solve life's mysteries, resolves significant problems).

WHERE TO FIND OUT MORE

International Association For Cryptologic Research: http://www.iacr.org/
National Security Agency: http://www.nsa.gov/careers/career_fields/cryptsiganalysis.shtml