Cryptography Lesson Plan

Overview - *Cryptography*

Summary

There is a large amount of sensitive information being stored on computers and transmitted between computers today, including account passwords, trade secrets, and personal financial information. To keep this information hidden from third parties who may want access to it, cryptographic techniques must be used to encrypt it, making it difficult or impossible to actually recover the original data for anyone but the intended recipient. Because most modern cryptographic algorithms involve high-level mathematical concepts, this activity will not discuss them, but it will investigate the general ideas behind cryptography and introduce the idea of analyzing the strength of different kinds of encryption.

Time Line

What	Time (mins)	Where
Introduction	5	Cryptography.pdf
Worksheet – The Caesar Cipher	10	CryptographyWorksheets.pdf
Class Discussion - Breaking Encryption	5	Cryptography.pdf
Party explanation	5	Cryptography.pdf
Encode surprise party	10	CryptographyWorksheets.pdf
Decode surprise party	10	CryptographyWorksheets.pdf
Wrap-up Discussion	5	Cryptography.pdf CryptographySlides.pdf (optional)
Total	50	

Materials

- ✓ Print the following handouts:
  - Worksheet 1: The Caesar Cipher, 1 per student
  - Worksheet 2: The Packet Villain, 1 per student
- ✓ (optional) Each student will need the following handouts:
  - Caesar Wheel (2 on each sheet)
  - May also be used just for class discussion, or omitted completely

Introduction to Cryptography

Cryptography is the study of encryption and decryption of messages. The principle of encoding a message is to ensure that only the intended receiver understands the message. Thus, when encoding a message, it is important to define a consistent “cipher”, which is known by the recipient beforehand. A “cipher” determines how the message is encrypted.

One of the earliest known ciphers is the Caesar cipher, which Julius Caesar used to send encoded and secure messages to generals in the Roman army. The Caesar cipher shifts the alphabet system by a predetermined amount so that the beginning letter of the encrypted messages alphabet is different than that of the original message. For example, a Caesar cipher that translates the message “BAD” into “EDG” is said to have a shift of 3. This is because each letter in the original message is shifted 3 letters forward in the alphabet. This cipher is relatively easy to break, due to the limited number of ciphers (25, to be exact), but is a good representation of the basic principles of cryptography.

Cryptography is widely used in computer science. Internet traffic is often encrypted at some level and relies on consistent cipher generation and transmission in order for secure messages to be sent.

The purpose of this module is to provide students an introduction into the world of cryptography through the Caesar cipher and to help students understand how cryptography is used in computer science.

Cheat Sheet

Terminology

Cryptography - the study of encryption and decryption of messages
Encoding- obfuscating a message
Decoding- figuring out the original message from the encrypted message

Introduction- Whole Class

Lesson Vocabulary (you may want to write on board)

- cryptography
- encode
- decode

Start by getting the students to think about what kinds of information might need to be kept hidden. What if all of our passwords were transmitted over the internet without any sort of encryption?

Take ideas about how we might protect sensitive information.

Next, explain the idea of encrypting a message (i.e., modifying it to be unrecognizable) before transmitting it to make it harder for someone who intercepts the message to actually read, unless they can figure out how to decode it. Then, transition into explaining the Caesar Cipher worksheet.

The following example will give students a good idea as to how cryptography works before they start the first worksheet. Tell the students you are going to encrypt a message using a cipher or "key" of size 2. Ask if they can decrypt the following message: eqorwvgt [**answer**: computer]

Activity- Worksheet 1: The Caesar Cipher

Worksheet – The Caesar Cipher

This worksheet introduces a very simple kind of encryption which was used by Julius Caesar. The worksheet walks the students through the mechanics of the cipher, and lets them practice using it on their own. Specifically, the allows students to sharpen their skills in encoding and decoding a variety of messages using different keys.

The Caesar Cipher Answer Key

Worksheet 1

The Caesar Cipher

Julius Caesar used a simple substitution cipher to send messages to his troops. He substituted each letter by the letter that was 3 places further along in the alphabet, so that “a” was replaced with “D”, “b” with “E” and so on.

Part I. complete the table below to show what each letter is enciphered as using this system.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Part II. Using the Caesar Cipher, encode the name of your school. Did your partner get the same answer?

____

Part III. Computer scientists would call 3 the “key” for this cipher. How many different keys are possible?

25

Part IV. Decode this message, which was encoded using the Caesar cipher from the table above:

w	h	a	t		d	o		y	o	u		g	e	t		w	h	e	n		y	o	u	
Z	K	D	W		G	R		B	R	X		J	H	W		Z	K	H	Q		B	R	X	

c	r	o	s	s		a		s	n	o	w	m	a	n		w	i	t	h		a	
F	U	R	V	V		D		V	Q	R	Z	P	D	Q		Z	L	W	K		D	

v	a	m	p	i	r	e	?		f	r	o	s	t	b	i	t	e
Y	D	P	S	L	U	H	?		I	U	R	V	W	E	L	W	H

Activity- Team Worksheet

Divide the class into groups of 3 or 4. Explain that each group is trying to get together a surprise party without the lucky person finding out. The team will need to make up the details - who will the surprise party be for? Where? What game or activity will you do at the party? What gift will you bring? You may want to encourage students to use answers that are fairly short (e.g., 1-3 words, not entire sentences)

Packet Villain. The first part of the worksheet is just to practice encoding/decoding when the exact cipher is not specified (but limited to one of 3, to keep it fairly simple). This exercise is called Packet Villain. This small practice should not take very long, but gives practice encoding a known message (the partner's name).

Surprise Party. Next the teams should encode the details of the party. Each person should encode only ONE detail. After the encoding is done, have the teams swap and see if they can figure out the details. Note that this will be harder, because students do not know a) which cipher was used or b) what the answer is.

If a team is really struggling, you might ask the other team to tell which cipher they used.

As teams finish the decoding, share some of the party details with the entire class.

What's It All About Discussion – Whole Class

People rely on encryption all the time when using the internet. Some of the uses of encryption include:

- Protecting credit card details or other sensitive information in online transactions.
- Protecting email communication from eavesdropping third parties
- Verifying the authenticity of software updates to prevent installation of malicious software

Without strong cryptographic algorithms, it would be impossible to hide information from others or verify the identity of anyone on the internet, and most of our modern internet infrastructure would not function.

A simple substitution cipher can be broken in fractions of a second by any modern computer. Modern cryptography uses the idea of computational *intractability* – problems which take unreasonable amounts of time to solve

Many algorithms are based on large prime numbers

- Multiplying two large primes: 15 microseconds
- Recovering the original two factors: 200,000 years

OPTIONAL: Modern decryption methods often rely on considering the context of encrypted words (i.e., what words come before and/or after) and also the frequency that different letters tend to occur in the English language. This material is covered in CryptographySlides.pdf.