Day 1

Introduction to Cryptology and Basic Ciphers

Activity	Suggested Time	Materials	Preparation/Summary
Scytale	5 min.	1 "tube" per 4 or 5 students, prepared scytale messages	Have the students try to decrypt the scytale messages.
Introductory remarks	20 min.	Journals, writing utensils	Discuss sending and receiving secret messages
Cipher Worksheet pt. 1	40 min.	Pens/pencils, worksheets, whiteboard/projector	Students work in groups to decrypt messages
Discussion	10 min.	Projector/whiteboard	Students present solutions
BREAK	15 min.		
Frequency analysis	45 min.	Books, networked calculators, worksheets	Students find the frequencies of words/letters and input them into tables
Compiling results	15 min.	Projector, graphing software	Class discussion of total data

Scytale

Have scytale enciphered messages prepared and "tubes" (paper towel rolls work well) ready. Tell the students that there is a hidden message on the papers and pass them out to groups of four or five students. After some time the students will probably become confused and discouraged, at this point hand out the tubes. It will probably not take long for someone in the class to try wrapping the paper around the tube. Mention the historical significance of the scytale.

Inroductory Remarks

Tell the students that the scytale is an example of a "cryptosystem" and explain what that means. Introduce the terms cryptology, cryptography, and cryptanalysis. Ask the students if they have ever sent or received secret messages and how they did it. Let them "think, pair, share" on this. Have them write a short passage in their journals of someplace they have seen secret messages used, how it was done, and why. Some may claim they don't know of any time they have heard of secret messages being used, be sure to remind them that signals in sports count for this.

Cipher Worksheet pt. 1

Hand out the cipher worksheet and explain that each message has been made secret in a different way. Have the students work in groups to decrypt each one. The first two should go very quickly. After a group finds a solution, halt group work for a moment so that group can present their solution at the board. If no groups manage to figure out the "rail fence," (and it will be very hard) give an example of plaintext and the associated ciphertext for a different rail fence and send them back to work. If the students make it to the substitutions, it will be very difficult for them. Do not give away too much right now as this will lead into the frequency analysis.

Frequency Analysis

Introduce the activity by saying that given the trouble everyone had with the substitutions on the worksheet the whole class should try to gather some additional information. Give each student a book (preferably a narrative or conversational piece in standard English, no textbooks/poetry). Have each student pick a "reasonable sample" of text (a short paragraph or equivalent) and count the occurrences of each letter in their sample on the Frequency Analysis worksheet. Also have them note any frequently used words. The students should input this data into the networked calculators which the instructor can display on the board via projector.

Compiling Results

Ask the students to "think, pair, share" about what they notice about the data. Compile these findings on the board. All students should note down these results (specifically frequently/infrequently used letters, general distribution pattern, and frequently used words) in their journals. Wrap up by asking the students to think about how this information could help them complete the worksheet in the next class.

Day 2

Frequency attacks and Crypto-machines

Activity	Suggested Time	Materials	Preparation/Summary
Warm up challenge	5 min.	Whiteboard/projector, pens/pencils, scratch paper	Students solve transposition ciphers
Security of transposition/substitution ciphers	30 min.	Journals, scratch paper, writing utensils	Introduce factorial and compare cipher security
Recall frequency analysis	10 min.	Pens/pencils, journals, whiteboard/projector	Review of the findings of the frequency analysis
Cipher worksheet pt. 2	30 min.	Pens/pencils, worksheets	Students work in groups to complete the worksheets
BREAK	15 min.		
Cipher disks	10 min.	Disk wheels, pins, scissors, projector, scratch paper	Students make and use cipher disks
Cipher Wheels	35 min.	Bottles, graph paper, construction paper, scissors, tape, projector, white board	Students make and use cipher wheels
Journal Writing	15 min.	Pens/pencils, journals	Students reflect on different cryptosystems

Warm Up Challenge

Post a few ciphertexts using transposition ciphers (at least one word scramble and one rail fence). Have the students solve these to remind them of what they learned the last day of class.

Security of Substitution/Transposition Ciphers

Ask the students to the figure out how many ways there are to scramble three, four, and five letter words. Note how there are not very many ways to hide small words in a message. Lead the discussion toward the pattern of factorial, and have the students note the definition of $n!$ in their journals. Note how many possible ways there are to assign the alphabet to a given cipher alphabet, and how this makes “brute force” unreasonable as a strategy to attack substitutions.

Recall Frequency Analysis

Display the results of the students’ frequency analysis. Have them “think, pair, share” about how to use this information to determine if a cipher is transposition or substitution. Have them TPS about how to attack a substitution cipher with knowledge of frequencies.

Cipher Worksheet pt. 2

The students can work in groups or on their own to crack the remaining ciphers on the worksheet. Patrol the room and check on their progress, asking questions. While the “Caesar shift” is probably the simplest cipher, it is also confusing for students as they will have to deal with the concept of one letter standing in for another. This is why it is left until last. After groups finish this ask if they notice a pattern to how the substitutions work. Try to lead them to figure out the nature of the Caesar shift.

Cipher Disks

Have the students make cipher disks and practice using them. Just so everyone is consistent, have the students use the outer wheel for the plaintext and the inner wheel for the cipher text. Note how the NSA disk pairs letters off, so if A is enciphered to Z then Z is enciphered to A. This makes it weaker than a standard Caesar shift. Have the students TPS about how one might change a cipher disk to improve its security.

Cipher Wheels

Have the students make and practice using cipher wheels. Assign a few students to rearrange the alphabet to make ten wheels, and randomly put them in order. Make sure everyone is using the same wheels and has them in the proper order. Directions should be displayed on the board at all times.

Journal Writing

Ask the students to reflect on the advantages and disadvantages of the various cryptosystems they have learned so far. In particular, they should reflect on how the cipher wheel is different than the other simple substitutions they have been shown.

Day 3

Polyalphabetic Ciphers

Activity	Suggested Time	Materials	Preparation/Summary
Warm up challenge	5 min.	Whiteboard/projector, pens/pencils, scratch paper	Students solve simple substitution ciphers
Analysis of the cipher wheel	15 min.	Journals, scratch paper, writing utensils	Determine the difficulty of cracking a cipher wheel
The Vigenere cipher	20 min.	Pens/pencils, vigenere cryptography worksheet, whiteboard/projector	Learn and practice using the vigenere cipher with the cipher disk
The matrix cipher	20 min.	Pens/pencils, matrix cryptography worksheets, whiteboard projector	Learn and practice using the matrix cipher
Journal writing	15 min.	Pens/pencils, journals	Compare the various polyalphabetic ciphers and their advantages
BREAK	15 min.		
Cracking the Vigenere	30 min.	Cipher disks, scratch paper, vigenere cryptanalysis worksheet	Students crack vigenere ciphers using a given interval
Rotory ciphers	30 min.	Cipher disks, pens/pencils, rotory cipher worksheet.	Students practice using their cipher disks as simple rotor machines

Warm Up Challenge

Post some simple substitutions, Caesar shifts are fine, for the students to work on. This will help remind them of what they learned the previous day of class.

Analysis of the Cipher Wheel

Have the students TPS about whether or not it is possible to use a frequency attack on the cipher wheel. Encourage the students to justify their answers and have the rest of the class TPS to verify their explanations. Have the students calculate how many ways there are to arrange their ten disks on the wheel. This will remind them of the factorial notation.

The Vigenere Cipher

Introduce the idea of using multiple substitutions with the cipher disk and have the students work through the vigenere worksheet. You can either use the NSA disks as is or have the students practice a “true” vigenere by turning the white outer disk over and looking through the paper. The worksheet assumes you are doing the latter but is easy to modify if you wish to do the former.

The Matrix Cipher

Introduce the matrix cipher and have the students work through the matrix cipher worksheet. This should go more quickly than before. Use any spare time you have to have the students TPS on how the matrix and vigenere compare as cryptosystems. Is one easier to use? Is one more secure? Why?

Journal Writing

Ask the students to write in their journals about which of the polyalphabetic ciphers they prefer. Which do they find easiest to use? Which is the most secure? Encourage the students to think and justify their answers.

Cracking the Vigenere

Have the students attempt to crack the vigenere ciphers that are on the vigenere worksheet. At first this may seem daunting to the students, encourage them to work in groups and try different approaches. If no progress is made point out that every letter in the keyword makes for a different substitution, and that simple substitutions can be attacked with a frequency analysis.

Rotory Ciphers

Demonstrate how the cipher disk can be rotated by a standard interval between each letter in a plaintext. While similar to a vigenere, the interval length is usually longer, it can be up to twenty six. Have the students use different rotations when they encipher their messages. As a question to think of at home, ask the students to consider which rotations will produce an interval of 26.

Day 4

The Enigma and Purple Ciphers

Activity	Suggested Time	Materials	Preparation/Summary
"Good" rotations	15 min.	Journals, pens/pencils, scratch paper	Students work out which rotations give a 26 interval for the rotor
Analysis of the rotor	15 min.	Journals, scratch paper, writing utensils	Students work to find the total number of "settings" for the rotor
Enigma and purple	30 min.	Computers, web browser	Read descriptions of the enigma/purple ciphers and use computer emulators
Journal writing	15 min.	Pens/pencils, journals	Describe various scenarios that would compromise a cryptosystem
BREAK	15 min.		
Cryptology Posters	50 min.	Poster paper, pens/pencils, markers/crayons/colored pencils, scratch paper	Students create posters illustrating various ciphers
Concluding Remarks	10 min.	N/A	Summarize the lessons and gather student feedback

"Good" Rotations

The students should work in groups to determine the precise answer to the question that was proposed last time: which rotations will give let the cipher disk land in all 26 possible positions? Most will try to "brute force" this, but eventually they will start to see a pattern forming. Have the groups share their work often and eventually the students should arrive at the correct conclusion (even if they do not phrase it this way): a rotation of length relatively prime to 26 will result in a 26 length interval.

Analysis of the Rotor

The students should work in groups to find out how many unique configurations there are for one rotor. Each configuration consists of a starting position and a rotation length. There are twenty six starting postions, and phi(26) = 11 good rotations, so the students should conclude there are 26 * 11 = 286 possible configurations. No doubt some groups will arrive at other answers. Ask questions of each group to make them justify their conclusions.

Enigma and Purple

Do a web search before class and find good resources for the students to peruse about the Enigma and Purple machines (http://www.cryptomuseum.com/crypto/enigma/index.htm is a good starting spot). There is a lot less available about Purple because it is not as famous, so you may have to resort to Wikipedia (which is an OK start point for this topic). Have the students read up and use an enigma simulator (you can find them through the first page).

Journal Writing

Have the students try to imagine ways in which a crypto system might be compromised that don't have to do with cryptanalysis such as
What if a ciphering machine falls into enemy hands?
What if the enemy finds out the encryption method we are using (i.e., substitution, vigenere, etc.)
What if a ciphertext and the associated plaintext fall into enemy hands?
How do we disseminate keys to everyone who needs them without the enemy getting them?
Which cryptosystems can overcome these problems and which cannot?

Cryptology Posters

The students should work in groups and make posters that illustrate the encryption methods for

1.) A transposition cipher (either a systematic word scramble or a rail-fence)
2.) A simple substitution cipher (feel free to let it be a shift or "picture" substitution)
3.) A keyword dependent polyalphabetic cipher (either matrix or vigenere)
4.) A rotory cipher (probably using their cipher disks).

Students' posters should illustrate the method for encipherment and decipherment, and then give an example ciphertext and the associated key for observers to decrypt for each cipher method. Float about the room and check on students' progress. You will find that groups will have wildly different ideas about how to show the information and what to give away. Some will hide answers or hints on the poster or even challenge the observer to crack the code without giving a key. A key should be given, but it should be allowed to use it as a hidden hint.

Concluding Remarks

Take some time to get feedback from the students. What did they find most/least interesting? Which activities did they learn the most from? What would they like to know about cryptology in the future? Any feedback from students is good to hear, so even if it is about your lessons and not about content necessarily encourage everyone to share.