Modern Cryptography
Activity 1:
Caesar Ciphers

Preliminaries: The Caesar cipher is one of the oldest codes in existence. It is an example of a substitution cipher, where each letter in the alphabet is replaced by another letter. In the Caesar cipher, the alphabet is shifted uniformly by some fixed number n. This integer becomes the key for both encoding and decoding messages. It is known as the Caesar cipher because Julius Caesar used this code (with a shift of 3) to encrypt his private notes.

Instructions: Select a short message to send to your partner and also select a shift value n. Using the cipher wheel, line up the letter 'a' on the interior circle with the n^{th} letter on the exterior circle and encipher your message one letter at a time. When you have finished encoding your message, pass the encoded message and the shift value to your partner.

Using the key you receive from your partner, rotate the cipher wheel until it matches up with their key. Then, use the wheel to decode their message one letter at a time.

Discussion: This method of encoding was used for more than 1000 years before it was broken by an Arabic mathemtician who formalized the notion of frequency analysis. The second table on page 4 shows the frequency that each letter in the English alphabet occurs in the Oxford dictionary. Think about the problems you see with this encryption method and why it is a poor choice for modern cryptography. What could be done differently to fix some of those problems?

Modern Cryptography
Activity 2:
Public–Key Cryptography

Preliminaries: The purpose of this activity is to gain some intuition for the idea of public key cryptography. Although we generally think of public–key cryptography in terms of mass internet communications, the same principles can be applied in many situations. A familiar example is a public mailbox slot, where anyone can deposit a letter, but only the owner has a key to take open the box and remove the letters. In this activity we will explore a more colorful interpretation.

Instructions: You have been provided with a blue pen and a black pen, as well as a blue piece of cellophane. The blue pen is your public key and the cellophane is your private key. Using either the blue or black pen, write a message to your partner. Then, sribble lightly over the text with both your black pen and your partner's red pen (public key). Exchange messages with your partner and try to decipher the message with the cellophane.

Discussion: Note that if a third party intercepts your message they will be unable to read it, even if they possess another copy of the public key (red pen) that was used to encode the message. Similarly, you are the only one that can read messages that have been encrypted with your public key (blue pen). No matter how many blue pens a cryptanalyst has, they will be unable to read your message. This is the key idea of public cryptography; that providing access to the message and public key doen not compromise the security of the encryption. How does this idea adress the concerns that we considered after the first activity?

Modern Cryptography
Activity 3:
RSA Algorithm

The purpose of this activity is to gain experience encoding and decoding messages with the RSA algorithm.

Setup: Your private key consists of the primes $p = 3$ and $q = 23$, so the number $3 \cdot 23 = 69$ will be the first part of your public key. Since $\varphi(69) = 2 \cdot 22 = 44$, we can choose $r = 5$. Since $5 \cdot 9 = 45 \equiv 1 \pmod{44}$, we have that $x = 9$. Thus your public key consists of $(69, 5)$.

Instructions: Choose a five letter word to be your secret message. Using the table provided, convert each letter to its numeric counterpart and record below. Write your public key on an index card and exchange cards with your partner. Encode your letters one at a time using your partner's public key and give the encrypted message to your partner.

Use your private key to decode the message that you receive. Enter the results in the table below and convert the message back to letters.

Outgoing Message

Letter	Number	Encoded Number

Incoming Message

Encoded Number	Number	Letter

Example Encoding:

Outgoing Message

Letter	Number	Encoded Number
B	2	$2^7 \equiv 63 \pmod{65}$

Example Decoding:

Incoming Message

Encoded Number	Number	Letter
52	$52^9 \equiv 16 \pmod{69}$	P

Modern Cryptography
Useful Tables

Alphabet Conversion Table

Letter	Number	Letter	Number
A	1	N	14
B	2	O	15
C	3	P	16
D	4	Q	17
E	5	R	18
F	6	S	19
G	7	T	20
H	8	U	21
I	9	V	22
J	10	W	23
K	11	X	24
L	12	Y	25
M	13	Z	26

English Frequency Analysis

Letter	Percentage
e	12.7%
t	9.1%
a	8.1%
o	7.5%
i	7.0%
n	6.7%
s	6.3%
h	6.1%
r	6.0%
d	4.2%
l	4.0%
c	2.8%
u	2.8%
m	2.4%
w	2.4%
f	2.2%
g	2.0%
y	2.0%
p	1.9%
b	1.5%
v	1.0%
k	0.8%
j	.2%
x	.2%
q	.1%
z	.1%