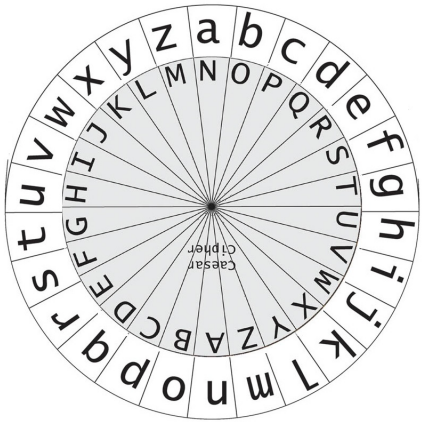
Modern Cryptography
Activity 1:
Caesar Ciphers

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 letter to represent the shift amount. Using the cipher wheel, line up the letter 'A' on the interior circle with the letter that you selected on the exterior circle. Encipher your message one letter at a time by finding the appropriate letter on the interior wheel and writing down the corresponding letter from the exterior wheel. For example, the picture below shows the case where the shift letter is 'n'. Under this shift, the letter 'P' is sent to 'c'.

When you have finished encoding your message, pass the encoded message and the letter you selected 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, this time reading from the outside wheel onto the inside wheel. In the example below 'g' would decode to 'T'.

Discussion: This method of encoding was used for more than 1,000 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?



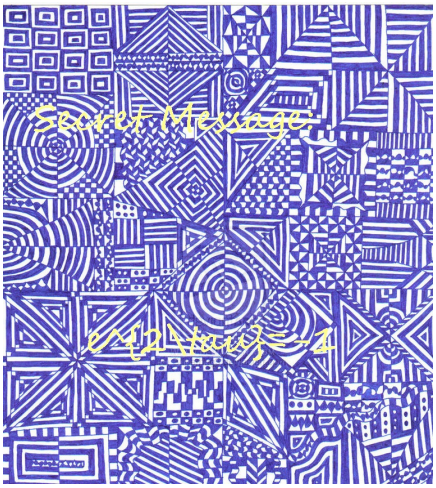
Modern Cryptography
Activity 2:
Public–Key Cryptography

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 the black pen, write a short message to your partner on an index card. Then, scribble lightly over the text with your black pen. Exchange public keys (colored pens) with your partner.

In order to encipher your message, scribble lightly over the index card with the red pen you obtained from your partner (their public key). Exchange encoded messages with your partner. Using the blue cellophane (your private key) try to decipher the message that you have received. More examples will be displayed on the projector and blackboard.

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 does not compromise the security of the encryption. How does this idea address the concerns that we considered after the first activity?



Modern Cryptography
Activity 3:
RSA Algorithm

Preliminaries: The purpose of this activity is to gain experience encoding and decoding messages with the RSA algorithm. These examples use very simplified choices of p, q, and r in order to make the computations feasible in our setting.

Setup: Your private key consists of the primes $p = 5$ and $q = 5$, so the number $5 \cdot 5 = 25$ will be the first part of your public key. Since $\varphi(25) = 4 \cdot 5 = 20$, we can choose $r = 3$. Since $3 \cdot 7 = 21 \equiv 1 \pmod{20}$, we have that $x = 7$. Thus your public key consists of $(25, 3)$. Write your public key on an index card and exchange keys with your partner.

Instructions: Select a message to send to your partner from the list below, The number to the right of the message is the plaintext that you will encrypt and send.

Math is fun!!	2
π is my favorite number.	3
$e^{2\pi i} = -1$	4
Cryptography is neat!!	6

Using your partner's public key, compute the ciphertext that corresponds to your message by raising the code number to the appropriate power modulo 25. Notice that since $4 \cdot 25 = 100$ we know that $100 \equiv 0 \pmod{25}$. This means that only the last two digits of the exponential that you compute are important. For example, $14^6 = 75,529,536 \equiv 36 \equiv 9 \pmod{25}$. This should make your computation simpler. Write the ciphertext that you have computed on an index card and give it to your partner.

Now it is time to decode the message that you have just received. Using your private key ($x = 7$), compute the original plaintext. This resulting number corresponds to the message that your partner sent.

More Decoding: Alice has sent you the following ciphertext message:

$$\{7, 9, 1, \ , 4, 9, \ , 16, 11, 19\}$$

The empty entries in the message represent spaces. Decode the message using your public key and the alphabet conversion table included on the next page.

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%

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 $p = 5$ and $q = 7$, so the number $5 \cdot 7 = 35$ will be the first part of your public key. Since $\varphi(35) = 4 \cdot 6 = 24$, we can choose $r = 5$. Since $5 \cdot 5 = 25 \equiv 1 \pmod{24}$, we have that $x = 5$. Thus your public key consists of $(35, 5)$.

Instructions: Choose a five letter word to be your secret message. Using the table provided, convert each letter to its numeric counterpart and enter it in the table 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	Decoded Number	Letter

Example Encoding:

Outgoing Message (using partner's public key)

Letter	Number	Encoded Number
D	4	$4^5 \equiv 10 \pmod{39}$

Example Decoding:

Incoming Message (using your private key)

Encoded Number	Number	Letter
12	$12^5 \equiv 17 \pmod{35}$	Q

Modern Cryptography
Activity 3":
RSA Algorithm

The purpose of this activity is to practice using the RSA public–key algorithm. The goal is to succesfully encode a message for your partners using their public keys and succesfully decode the messages that you receive using your private key.

(1) Choose a 5 letter word: _____
(2) convert each letter to a number using the provided chart:
   (a) _____ → _____
   (b) _____ → _____
   (c) _____ → _____
   (d) _____ → _____
   (e) _____ → _____
(3) Your primes are 7 and 13. Notice that $7 \cdot 13 = 91$ and that $\varphi(91) = 6 \cdot 12 = 84 = 3^2 * 2^3$. This lets us choose $r = 5$ and we can find $x = 17$ since $5 \cdot 17 = 85 \equiv 1 \pmod{84}$.
(4) Write your public key: $(91, 5)$ on an index card and reveal it to your partners.
(5) Copy your partner's public key here $pq =$_____ $r =$_____
(6) Using your partner's public key encrypt your message one letter at a time. For example if their public key is $(15, 7)$ and your first letter is $b \to 2$ compute $2^7 = 128 \equiv 8 \pmod{15}$ and write $2 \to 8$.
   (a) _____ → _____
   (b) _____ → _____
   (c) _____ → _____
   (d) _____ → _____
   (e) _____ → _____
(7) Write the encoded numbers on an index card and hand them to your partner.
(8) Write the five encoded numbers you received:
   (a) _____
   (b) _____
   (c) _____
   (d) _____
   (e) _____
(9) One at a time, decode these numbers using your private key. For example, if you recieve the number 4, compute $11^{17} = 17179869184 \equiv 23 \pmod{91}$.
   (a) _____ → _____
   (b) _____ → _____
   (c) _____ → _____
   (d) _____ → _____
   (e) _____ → _____
(10) Finally, using the provided chart transform the deciphered message back to letters:
   (a) _____
   (b) _____
   (c) _____
   (d) _____
   (e) _____