Cryptography

_____ is the study of sending information securely despite the presence of eavesdroppers. _____ is the message you want to send in plain English. _____ is a method of modifying the plaintext (or encrypting) so that it cannot be understood by an eavesdropper. _____ is the encrypted plaintext. _____ is a tool used in order to encrypt the plaintext, and to decrypt the ciphertext.

Caesar Ciphers

Here is how the Caesar cipher works:

The shift is the _____.
First we turn our message into _____ using the following table:

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Once our plaintext is turned into numbers, we encrypt by
_____ and _____
If one of the numbers is bigger than 25 we
_____

An example of a Caesar cipher is:
Key =

Plaintext:	**KITTY**
PT in Numbers:	
+Key:	
mod 26:	
Ciphertext:	

Your turn to encrypt! What is your favorite flavor of cake?

Key= **5**

Plaintext:	
PT in Numbers:	
+Key:	
mod 26:	
Ciphertext:	

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

We decrypt a Caesar cipher by _____

An example of decrypting a Caesar cipher is:

Key=

Ciphertext:	**DNTPYNP**
CT in Numbers:	
-Key:	
mod 26:	
Plaintext:	

Your turn to decrypt! The answer to the following has been encrypted: What do you call a destroyed angle?

Key=

Ciphertext:	**BOMDKXQVO**
CT in Numbers:	
-Key:	
mod 26:	
Plaintext:	

Public Key Cryptography

In **private key cryptography**, the keys are shared _____. This makes encryption less secure, because _____.

In **public key cryptography**, any part of the key that gets shared is shared _____. Describe how this could be done for paint.

The **Diffie-Hellman key exchange** is a method of exchanging keys over public channels. If Alice and Barb want to share a key:

1. Alice and Barb agree on _____
2. Alice chooses a secret integer a and sends Barb _____
3. Barb chooses a secret integer b and sends Alice _____
4. Alice computes _____
5. Barb computes _____
6. Alice and Barb share the key _____

Here is an example of sharing a key using Diffie-Hellman: