Cryptography

What Is Cryptography?

Cryptography is the study and techniques of sending information safely and securely. That is, if the message is sent, and intercepted, then the message will remain unread. Cryptanalysis is the study of finding the hidden information.

Why Would We Need Encryption?

Very often, we want to send information without allowing others to have access to the information. You use encryption almost every day while using the Internet or buying items.

- Verify who we are communicating with.
- Prevent others from altering our communication.
- Protect our identity.
- Keep our banking information secure.

What other things do we use encryption for?

Caesar Cipher

We are going to use the Caesar Cipher. You have all received a paper with two circles, one smaller than the other. You are going to cut out the circles and pin them together to make a wheel. From here we are going to be able to generate new alphabets by shifting the smaller wheel around and replacing the letters of you message with the corresponding letter on the smaller wheel.

Make a Code

Try coming up with a sentence which you will encrypt using the Caesar Cipher and pass to another group with give the key. Give them another sentence that you have encrypted, but do not give them a key . This means you will be receiving an encrypted code, for which you do not have the key. Is there any way to know what that message is?

Break a Code

What if you didn't have a key? Would you still be able to find the information? Try and see if you can crack this cipher. Try it without using your newly crafted wheel.

```
Rw. fsi Rwx. Izwxqjd, tk szrgjw ktzw, Uwnajy Iwnaj, bjwj uwtzi yt
xfd ymfy ymjd bjwj ujwkjhyqd stwrfq, ymfsp dtz ajwd rzhm. Ymjd
bjwj ymj qfxy ujtuqj dtz'i jcujhy yt gj nsatqaji ns fsdymnsl
xywfslj tw rdxyjwntzx, gjhfzxj ymjd ozxy inis'y mtqi bnym xzhm
stsxjsxj.
```

Anything Better?

Yest there is! So far we have only talked about what is called symmetric keys, that is, we

both have the same key. What if you have the key and want to send me the key without others having access to it? Surprisingly, we can do this. One such method is called RSA, and though we do not have the time to explore this topic, I encourage you to learn more about it at Khan Academy or other online resources.