New Topics for Junior High Mathematics (2012-2013)

Cryptography [1]

Cryptography is the mathematics behind secret codes and messages. The use of cryptography began thousands of years ago and continues to be used today. Anytime you click "submit" or "send" on a computer screen that contains your username and password or the PIN to your bank account, you can thank cryptography and be assured that your data is being safely sent across the internet.

The purpose of cryptography is to communicate from person to person in such a way so that if the message is intercepted, it cannot be read by the third-party. To conceal a message with cryptography, the message must first be **encrypted**. If the message is intercepted by a third-party, the message will not have any meaning since the encrypted message does not resemble the original message. When the recipient gets the message, he must then **decrypt** the message to get its meaning.

One **cipher** used to conceal the true meaning of a message is the shift cipher. In an N-**shift cipher**, each letter of a message is encrypted by replacing it with a letter that is N letters ahead of it in the alphabet. Letters at the end of the alphabet are encrypted by rolling back around to A, B, etc. One common shift cipher is the **Caesar cipher**, which is a 3-shift cipher, moving letters 3 ahead.

Caesar cipher

plaintext	**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**
ciphertext	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Using the Caesar cipher, we use the table above to encode **plaintext** into **ciphertext**. The word **CAT** is encrypted into **FDW**, since **C** $\longrightarrow$ **F**, **A** $\longrightarrow$ **D**, and **T** $\longrightarrow$ **W**. In reverse, if you are given the ciphertext **PDWK**, this word can be decrypted as **MATH**, since **P** $\longleftarrow$ **M**, etc.

Other shift ciphers can be used, based on how far the letters are shifted over. Here is the table giving the 5-shift cipher:

plaintext	**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**
ciphertext	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**

Notice that under the 5-shift cipher, the word **CAT** is encrypted as **HFY**.

Another type of cipher is a **substitution cipher**, where each letter is encrypted to another letter and each letter is used exactly once. Here is an example of a substitution cipher:

plaintext	**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**
ciphertext	**H**	**R**	**U**	**J**	**Y**	**D**	**E**	**B**	**S**	**K**	**X**	**N**	**I**	**P**	**Q**	**L**	**Z**	**O**	**G**	**M**	**V**	**F**	**W**	**A**	**T**	**C**

To encrypt the word **DOG** using this substitution cipher, we would have **JQE**. Notice that in this cipher, **W** $\longrightarrow$ **W**; a letter does not necessarily need to be mapped to a different letter.

[1] This document was prepared by Doug Ray for competition, 2011-2013. If you have any questions about the material presented, please email doug@academicmeet.com.

Breaking Ciphers

Breaking ciphers is extremely challenging. Think about it. If it were easy to break a cipher, then you would not want to send private information, like your banking PIN number, over the internet. It would be too easy for other people to obtain the information and decipher the code. However, given certain conditions, it is possible to make reasonable guesses to decrypt a cipher.

If you have been given a message that contains one-letter words, then those words are probably the words "a" or "I." Also, if you know that you have been given a message encrypted through a shift cipher, simply try to decrypt the message using a shift cipher that would encode "a" to the one-letter word or try the shift that would encode "I" to the one-letter word. Decoding other words with this cipher will check the validity of your choice.

Suppose you are given the ciphertext **L ORYH FUBSWRJUDSKB**. The one-letter word **L** is probably either **A** or **I**. Trying to decrypt the message using **L** ⟵ **A** gives **A DGNW UJQHLGYJSHZQ**, which is clearly not the original message. However, using the shift that decrypts **L** ⟵ **I**, the decrypted message turns out to be **I LOVE CRYPTOGRAPHY**.

Sample Problems

Use the following ciphers and the Caesar cipher (previous page) to solve these problems.

8-Shift Cipher

plaintext	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
ciphertext	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

12-Shift Cipher

plaintext	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
ciphertext	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

Substitution Cipher

plaintext	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
ciphertext	P	I	K	C	V	M	L	S	E	J	Q	Y	H	G	F	A	B	N	T	U	O	D	Z	W	X	R

---

1. Encrypt **FISH** using the Caesar cipher.
2. Encrypt **PET** using the 8-shift cipher.
3. Encrypt **HORSE** using the 12-shift cipher.
4. Encrypt **CAR** using the substitution cipher.
5. Decrypt **EDUN** using the Caesar cipher.
6. Decrypt **YQAI** using the 12-shift cipher.
7. Decrypt **TPEY** using the substitution cipher.
8. Determine the shift used to encrypt the message into **I ZML NWF ZIV IKZWAA BPM ZWIL** and decrypt the message.
9. How many different shift ciphers are there (not counting the 0-shift cipher which does not change any of the letters)?
10. How many substitution ciphers are there?
11. What role did cryptography play in both World War I and World War II?