Day__ # Cryptography Name_____

What is cryptography and why do we need it?

Cryptography is the study of means of converting information from its normal, understandable form into an understandable format, rendering it unreadable without secret knowledge.

Using strong encryption techniques, sensitive, valuable information can be protected against organized criminals, malicious hackers, or spies from a foreign military power, for example. Indeed, cryptography used to be almost exclusively a tool for the military. However, in moving into an information society, the value of cryptography in everyday life in such areas as privacy, trust, electronic payments, and access control has become evident. In this way, the field of cryptography has broadened from classical encryption techniques into areas such as authentication, data integrity, and non-repudiation of data transfer.

In today's information society, cryptography has become one of the main tools for privacy, trust, access control, electronic payments, corporate security, and countless other fields.

The use of cryptography is no longer a privilege reserved for governments and highly skilled specialists, but is becoming available for everyone.

Some definitions

Ciphers

> Ciphers are the oldest and simplest to understand. Ciphers take one character of a source document and convert it to a different character in the destination document. It can do this by converting one character into another, by moving the characters around within the document, or by a combination of both.

Codes

> Codes are a logical extension of ciphers in that whole words, phrases, dates, etc. are converted to a new sequence in the encrypted text.

Decryption

> Decryption is the process of converting coded text into the original plain text.

Encryption

> Encryption is the process whereby plain text is converted into an encoded (or encrypted) text.

Lumping Words (format)

Get rid of spaces and returns to lump words together. Use upper case letters to make the code harder to read and decode.

IBETTHISISHARDFORMANYPEOPLE.

Answer: I BET THIS IS HARD FOR MANY PEOPLE.

You try one:

CANYOUREADTHISMESSAGE

Answer: _____

Character Blocks

Block letters of a message by 2, 3, or more characters.

IL IK EI CE CR EA M.

After combining all of the letters above you get "ILIKEICECREAM." Looking for words in the message you'll find "I LIKE ICE CREAM."

You try one:

DRI NKI NGW ATE RIS GRE AT

Answer: _____

Backwards English

Writing words, sentences, or entire message backwards can be very confusing!

EES UOY TA EHT EROTS.

Reading EES backwards yields the answer SEE. The answer to this encrypted message is "SEE YOU AT THE STORE."

You try one:

I EVOL GNITAE A TIURF RO EIGGEV

Answer: _____

Selected Characters

Choose a mathematical algorithm or pattern to create or decipher a secret message from a plain message. This example uses a pattern to make a secret message: *D* id *e* veryone *a* t *t* he *h* ouse … etc. "DEATH" is the secret message with the words in this message. You try one:

Did every student start eating red tomatoes? Surely, all remembered eating our vegetables. Even Randy Robinson ate tomatoes every day.

Answer: _____

Alphabet Wheel

An alphabet wheel, often called a cipher clock, is a graphical picture of values that can be used to represent the letters of the alphabet. Most wheels have the plain alphabet in the inside of the circle and the cipher alphabet on the outside. Below is an example. Using the picture below, you can see that the letter "A" inside the circle (from the original message) is equal to the cipher character "G." Thus you would write the phrase "PROTEIN IS YUMMY" as:

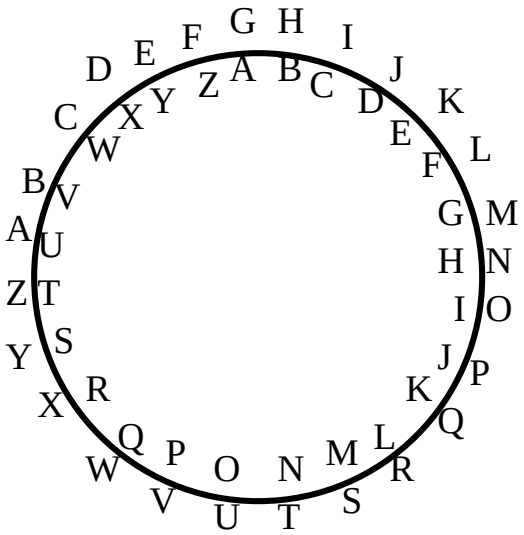
VXUZKOT OY EASSE

You try to put one in code:

I LOVE SCRAPPLE = _____

Now try to decode this:

JUMY GXK MXKGZ VKZY = _____



Alphabet and Word Correlated Ciphers

Sometimes keywords are used to help encipher and decipher a message. By writing out a sentence(s) that contains all the letter of the alphabet, which is called the keyword phrase, you can correlate plain alphabet letters to letters within a word found in the keyword phrase.

The keyword phrase below contains all the letters of the alphabet. Some of the letters are used more than once in the phrase. You can also make up your own.

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
1 2 3 4 5 6 7 8 9

To encipher:
Each letter is represented by a two-digit number. First, you find the word in the keyword phrase that contains the message letter. Then you write down the number of the word, followed by the number of the letter in the word. For example, the number 82 would represent the letter "A", because A is the 2nd letter in the 8th word.

For example:

J	O	H	N	S	O	N		I	S		A		S	P	Y
51	33	12	35	55	33	35		23	55		82		55	54	84

Since some of the letters in the keyword phrase repeat, you can use different numbers to represent the same letter. For example, the letter "O" could be represented by 33, or 42, or 61, or 92. Any are acceptable to use.

You try to put one in code:

PICTURES ARE FUN TO TAKE=

_____

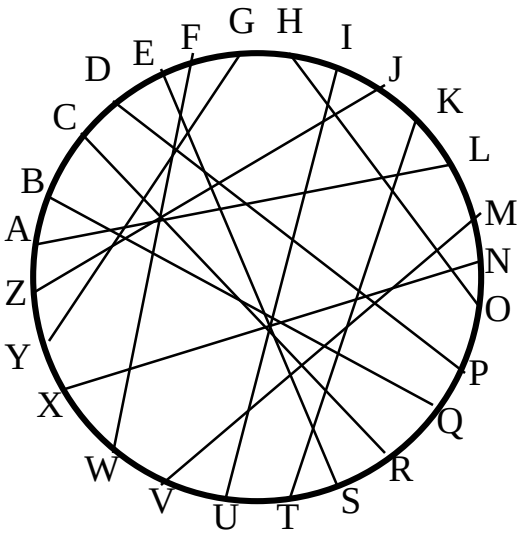
Now try to decode this:

23 81 23 25 73 11 92 64 63 82 91 31 61 42 25 55 =

_____

Letter Spokes Cipher Clock

The letter spokes cipher clock resembles the spokes of a wheel. It's another way of making up a random alphabet substitution wheel. Simply take each letter in the wheel and line it up with another letter somewhere else on the wheel by using a line to connect the two. If you get an encrypted message, use the letter spokes cipher clock to find the letter tied to the encrypted letter.



For example, "PANDAS LIKE BAMBOO" would be written as "DLXPLE AUTS QLVQHH."

You try to put one in code:

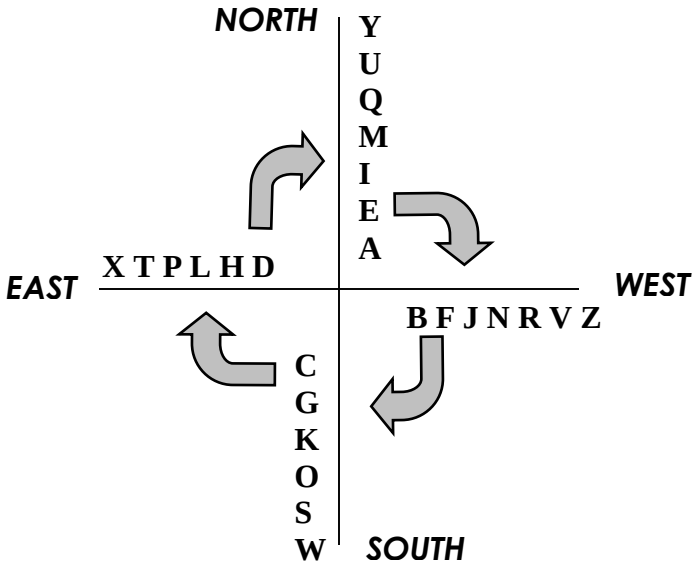
WATER IS GOOD FOR YOU = _____

Now try to decode this:

ALIYO VHCS LXP OLMS WIX = _____

Compass Cipher

The compass cipher makes use of a well-known pattern, the directions of north, south, east, and west. There are lots of ways to create a compass key. One way, as shown below, is to make a cross in the center of your paper and write out the letters of the alphabet along each line, spiraling outwards.



Once you have all the letters written into your compass, write out the letters from outside in and then combine all of the letters into a long line. Finally, write out the plain alphabet below it to come up with an alphabet substitution cipher. Looking below, you can see that the word "CAT" would be written as "QYB"

NORTH: YUQMIEA
SOUTH: WSOKGC
WEST: ZVRNJFB
EAST: XTPLHD

Compass Key: Y U Q M I E A W S O K G C Z V R N J F B X T P L H D (in NSWE)
Alphabet: 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

You try to put one in code:

GHOSTS ARE SCARY = _____

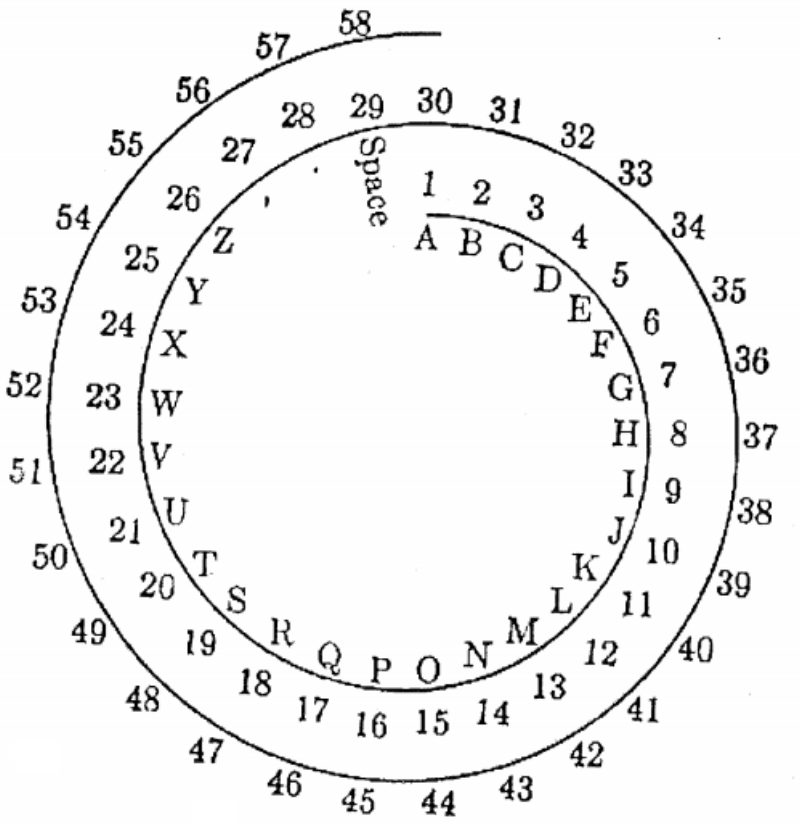
Now try to decode this:

ZVP S XZMIJFBYZM = _____

Spiral Cipher Clocks

To make a cipher clock even harder you may want to create a spiral cipher that gives each character on your cipher clock multiple values. The picture below shows a spiral cipher clock with letters A-Z, a comma, period, and a space. Each character on the clock can be represented with a number. In the first spiral, the letter A is equal to 1, B is equal to 2, and so on.

As the spiral continues around the cipher clock each character is given another value that ***<u>can</u>*** **be used** in your cipher. A is also equal to the number 30, in the second spiral.



You try to put one in code:

SHOWERS MAKE YOU CLEAN = _____

Now try to decode this:

12 34 30 18 14 9 43 7 29 38 19 58 35 21 14 =

_____

Vigenere Method

The Vigenere Method is very difficult to break. A key word is used to encipher the message.

To encipher:
A message is written out with the key word written above it repeatedly. Then correlate the key word letter with the message letter using the Vigenere Table on the next page. To do this, look for the keyword letter in the far left column of the table, and the corresponding message letter in the top row of the table. Then, find the encrypted letter that corresponds to where the row of the message letter and column of the keyword letter meet.

Look at the example below to see how to encipher messages.

Keyword: CASH
Message: THIS IS COOL

Keyword Letters:	C A S H	C A	S H C A
Message Letters:	T H I S	I S	C O O L
Enciphered Letters:	V H A Z	K S	U V Q L

Notice how the keyword CASH is written above the message. Then we correlate the keyword letter with the message letter on the Vigenere table. Following the key word column "C" down to the message letter row "T" you find the enciphered letter "V."

You try to put one in code:
Use the same keyword as above: CASH

THE SUN IS BRIGHT = _____

To decipher:
To decipher, you need to know the keyword. Again, write the keyword above the enciphered message. Then look for keyword letter in the far left column. Once you find it, scroll across the row until you see the enciphered letter in the middle of the table. Once you find it, look up that column to find the message letter in the top row.

Now try to decode this:
Keyword: LOGIC

TG ZPKD RONHTQATV? = _____

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

Bifid Cipher

The Bifid Cipher is a type of matrix, or columnar transposition, cipher. Start by creating a 5 by 5 matrix of letters, with the rows and columns labeled 1 to 5.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y Z

To start, find the value of each letter by reading the row and the column values. The two numbers are then written vertically on a piece of paper below the plain letter. All the plain letters within the secret message are written next to one another as seen below:

Plain Message:	S E N D	R E I N F O R C E M E N T
Row Value:	4 1 3 1	4 1 2 3 2 3 4 1 1 3 1 3 4
Column Value:	4 5 4 4	3 5 4 4 1 5 3 3 5 3 5 4 5

Notice how the letter "S" has the value of 44. "E" is 15 since it is found in row 1, column 5. Y and Z share the position of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, you rewrite the message from left to right, combining numbers into groups of 2.

41 31 41 23 23 41 13 13 44 54 43 54 41 53 35 35 45

The last step is to take each group of numbers, such as 41 and 31 in the beginning of the line above, and find the corresponding cipher values in the same matrix above. 41 is row 4, column 1, the letter "P." See if you can finish filling in the cipher letters below:

41	31	41	23	23	41	13	13	44	54	43	54	41	53	35	35	45
P	K	P	H	H	P	C	C	S	X	R	X	P	W	O	O	T

So the message "SEND REINFORCEMENT" turns into "PKPHHPCCSXRXPWOOT."

Now you try this one: I LOVE TO RUN = _____

To decode:

Work backwards! Let's try this one:

I I H QL W X X R Y S U J

First, take the encrypted letters and find their two digit numbers.

I	I	H	Q	L	W	X	X	R	Y	S	U	J
24	24	23	42	32	53	54	54	43	55	44	51	25

Now, count how many letters you are supposed to have. In this example, you have 13 letters in your encoded message, so you will have 13 letters in your decoded message. Thus you need to have two rows of 13 numbers. So in working backwards, we need to write the first 13 numbers on the top row and the next 13 numbers below in the second row. For our example:

2	4	2	4	2	3	4	2	3	2	5	3	5
4	5	4	4	3	5	5	4	4	5	1	2	5

Now we must find the corresponding letters for each number. In our example:

I	T	I	S	H	O	T	I	N	J	U	L	Y
2	4	2	4	2	3	4	2	3	2	5	3	5
4	5	4	4	3	5	5	4	4	5	1	2	5

So the message is "IT IS HOT IN JULY."

Now you try this one:

F L O B C K L H I Z W D T T Z M B J Q S F E V X =

Transposition Cipher

For an example of a transposition, suppose Alice wants to send Bob the message:

THIS IS FUN!

Write your message on two lines, alternating writing one letter on the top line, the next letter on the second line, until the entire message has been written.

Line 1: T I I F N
Line 2: H S S U !

Then write out your message by writing out the characters from the first line in order and then second line in order. So for our example: TIIFNHSSU!

Now you try encrypting one:

I REALLY LOVE INDE AT CTY = _____

To decipher:
Count the number of letters and divide by 2. Then, arrange the letters into two columns. Let's look at the following example.

T L V S O I E T R A N N E E I I N S N E T I I G = 24 characters;
24 characters / 2 = 12 letters per line.

Put the first half of the letters on the top line, and the second half on the second line.

Line 1: T L V S O I E T R A N N
Line 2: E E I I N S N E T I I G

Then write out the letters by alternating between line 1 and line 2.

T E L E V I S I O N I S E N T E R T A I N I N G
Line # 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2

So the decrypted message would be: Television is entertaining.

Now you try to decipher the following message:

PRITNENHRWRMKSSMREESSECADADOKAEUSATR =

_____

Double Transposition Cipher

Double Transposition consists of applying a columnar transposition to a message. Columnar transposition works like this: First pick a keyword, such as DESCRIBE. Then write the message under it in rows:

```
D E S C R I B E
---------------
Y O U R M O T H
E R W A S A H A
M S T E R A N D
Y O U R F A T H
E R S M E L T O
F E L D E R B E
R R I E S Z Z Z
```

If there are spaces in the last row (like there are above) fill them with Z's.

Now number the letters in the keyword in alphabetical order. If a letter repeats (like 'E' in DESCRIBE), then number the repeated letter from left to right.

```
3 4 8 2 7 6 1 5
D E S C R I B E
---------------
Y O U R M O T H
E R W A S A H A
M S T E R A N D
Y O U R F A T H
E R S M E L T O
F E L D E R B E
R R I E S Z Z Z
```

Then read the cipher off by columns, starting with the lowest-numbered column: Column 1 is THNTTBZ, followed by RAERMDE YEMYEFR ORSORER HADHOEZ OAAALRZ MSRFEES UWTUSLI.

You encipher this message using the keyword SHOES:

PAY ME BY SUNDAY OR SUFFER THE CONSEQUENCES.

To decipher:

To decipher a message, you need to know the keyword. Let's try the following message:

NEOYAZDWSSYERAOTDDITYARZKRUHTZ
Keyword: HOWDY.

Since the Keyword has 5 letters, you will have 5 columns. Each column will have the same number of letters in it (since we fill any spaces with Z's). Thus, we must count the number of letters and divide by 5. That will let us know how many letters are in each column.

NEOYAZDWSSYERAOTDDITYARZKRUHTZ = 30 letters
30 / 5 = 6 letters per column

Next we separate the encrypted message into groups of 6 letters.

NEOYAZ DWSSYE RAOTDD ITYARZ KRUHTZ

Next, we will alphabetically order the keyword: DHOWY. Now, write each group of 6 letters of the code vertically underneath the letter:

D	H	O	W	Y
N	D	R	I	K
E	W	A	T	R
O	S	O	Y	U
Y	S	T	A	H
A	Y	D	R	T
Z	E	D	Z	Z

H	O	W	D	Y
D	R	I	N	K
W	A	T	E	R
S	O	Y	O	U
S	T	A	Y	H
Y	D	R	A	T
E	D	Z	Z	Z

Now, rearrange the keyword and write out the message left to right:
DRINK WATER SO YOU STAY HYDRATED.

Now you try this one:
AEGIRCAOHPARDSZNSOTUPKEWY
Keyword: WATER