



University of Waterloo
Faculty of Mathematics



Centre for Education in
Mathematics and Computing

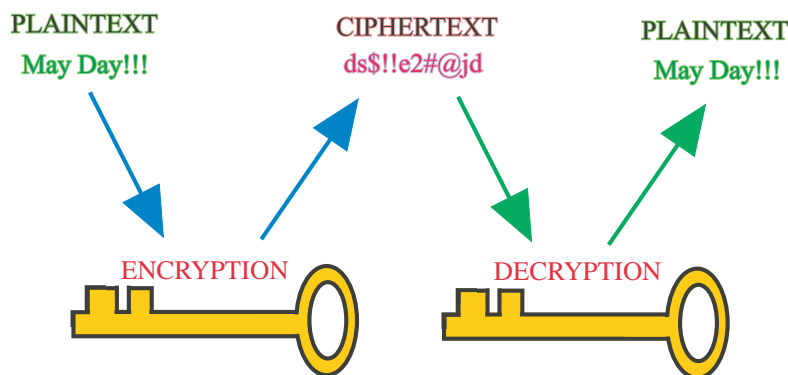
Grade 7 & 8 Math Circles February 9, 2011 Cryptography and Binary Numbers

Q: What did the teddy bear say to the waiter when he offered the dessert menu?

A: CD JASCIH, T SB HJKZZYW!

How does cryptography work?

Using a **key** to **encrypt** the message, also known as **plaintext**, the sender gives the receiver the “scrambled message”, also known as **ciphertext**. Then, the receiver can use the key to unscramble, or **decrypt** the ciphertext back to plaintext to read the message!



Substitution Cipher

Substitution cipher is a method of encryption where each letter in the alphabet is associated with a unique letter, word, or even symbols. The key to the encryption can be written in the form of a table. We can have different substitution ciphers for the same message. For example, let's say we want to encrypt the following message:

I LIKE TOAST

Caesar Cipher: Pick a number between 1 and 25. We are now going to shift the whole alphabet to the right so that each letter is replaced by a letter of a fixed distance.

Number: 8

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

Ciphertext: A D A C W L G S K L

Exercises:

1. Encrypt "MATH CIRCLES" using Caesar cipher with the number 5.

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

Ciphertext: H V O C X D M X G Z N

2. Decrypt "KLJPWOLY AOPZ!!" using Caesar cipher with the number 19.

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

Plaintext: D E C I P H E R T H I S

Keyword Cipher: Pick a word with no repeating letters, and write each letter into the first boxes. Then, fill in the remaining boxes with the letters we haven't used yet in alphabetical order.

Keyword: **THANKS**

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

Ciphertext: D G D F K R L T Q R

Exercises:

3. Encrypt the phrase "I THINK I CAN" using keyword cipher with the word "vector".

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

Ciphertext: D Q B D J G D C V J

4. Decrypt "JHSB CR OTK!!" using keyword cipher with the word "hexagon".

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

Plaintext: M A T H I S F U N

Combining Ciphers: We can make a message more secure by combining ciphers. For example, we can encrypt a plaintext into ciphertext using Caesar cipher, and then treat that ciphertext as plaintext and encrypt it again using a keyword cipher.

Exercises:

- “What do monsters read when they want to know their future? ESEPVRQHBNFS!!!” The answer was first encrypted using keyword cipher with the keyword “crypto”. Then, it was encrypted again using word shift cipher with the word “circle”. Decrypt the cipher to find out the answer!
- The secret answer at beginning was encrypted twice using two different substitution methods. Decrypt the cipher to find out what the teddy bear said! (*Hint: when using keyword cipher or word shift cipher, use the word “matrix”*)

7. “Cipher Number” 5 19 5 16 22 18 17 8 2 14 6 19
 Word: CIRCLE → 3 9 18 3 12 5 3 9 18 3 12 5
 BJMMJMNYJKTN ← 2 10 13 13 10 13 14 25 10 11 20 14

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

Plaintext: HORRORSCOPES

- The proper decryption is to use keyword cipher, then Caesar cipher with a key number of 20

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

CD JASCIH, T SB HJKZZYW → HI NBUHEM, C UG MNOZZYX

After the Caesar shift, the plaintext says “NO THANKS, I AM STUFFED!”

Binary Numbers

Most cryptography today are done on computers because computers do the tedious calculations for us. Computers store information in a **base-2** system. What this means is that information is represented as a chain of 1's and 0's on the computer. This is the **binary system**. Our “normal” number system is the base-10 system. We are going to use the binary form of numbers in order to encrypt the message:

DRINK MILK

But first, let's learn how to convert between our usual numbers and binary!

Binary to Base-10 Let's say we want to convert the binary number 10110 into base-10,. We first write out the powers of 2.

$$2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 16 \quad 2^5 = 32$$

Going from right to left, the first “digit” of a binary represents 2^0 , the second “digit” represents 2^1 , the third represents 2^2 and so on. With this idea, we can write 10110 as

$$(1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) \text{ which is equal to } 16 + 4 + 2 = 22$$

Base-10 to Binary Let's say we want to convert the number 27 into binary. We need to write out 27 in the form $(a \times 2^4) + (b \times 2^3) + (c \times 2^2) + (d \times 2^1) + (e \times 2^0)$ where a, b, c, d and e are either 1 or 0. To do this, we find the largest power of 2 that is less than 27. In this case, it is 16. Then we find the difference: $27 - 16 = 11$. We then repeat the process until we get a difference of zero.

$$\begin{array}{ll} 27 - 2^4 = 11 & \rightarrow a = 1 \\ 11 - 2^3 = 3 & \rightarrow b = 1 \\ 3 - 2^1 = 1 & \rightarrow c = 0 \text{ and } d = 1 \\ 1 - 2^0 = 0 & \rightarrow e = 1 \end{array} \quad \begin{array}{l} \text{This gives us} \\ 27 = (1 \times 2^4) + (1 \times 2^3) + (0 \times 2^2) + (1 \times 2^1) + (1 \times 2^0) \end{array}$$

So, we can write 27 as 11011 in binary. (Note that 27 can be written as 11011, 011011, 0011011, 00011011,...)

Exercise:

9. Complete the table.

Base-2	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	Base-10
011011	0	1	0	0	1	1	27
000101	0	0	0	1	0	1	5
001011	0	0	1	0	1	1	11
100101	1	0	0	1	0	1	37
010010	0	1	0	0	1	0	18
100100	1	0	0	1	0	0	36
110110	1	1	0	1	1	0	54

Now we have enough background knowledge to learn about this next encryption method!

Block Cipher

Unlike the other ciphers we have covered, this method breaks letters and spaces into equal blocks (hence its name). Also, the letters are no longer associated with a distinct symbol anymore. Let's go back to our example "DRINK MILK": Similar to the word shift cipher, we need to convert each letter into a number according to its position in the alphabet. We also convert the spaces in between words into 0.

DRINK MILK \longrightarrow 4 18 9 14 11 0 13 9 12 11

Now, we convert each number into binary so the result is one long chain of 1's and 0's. Each number should have a length of 5 digits (eg. 27 would be 11011, not 011011).

00100100100100101110010110000001101010010110001011

Next, we pick a number and split the long chain into groups of that number. If the last group is missing digits we can fill it in with 0's; this technique is known **padding**.

Number: 4

0010 0100 1001 0010 1110 0101 1000 0001 1010 1001 0110 0010 1100

Now, we convert from binary back into base-10!

Ciphertext: 2 4 9 2 14 5 8 1 10 9 6 2 12

Exercise:

10. Encrypt a phrase or a word using block cipher and exchange with another to decrypt their ciphertext. Remember to tell each other the key number!

Chaining: This last encryption method combines the concept of blocks and word shift. Let's encrypt the phrase "DRINK MILK" again. Pick a word and note the numbers of letters in that word (this will be our "key number").

Word: MOO

Number of letters (key number): 3

Replace any spaces with a symbol (e.g. a space can become @)

DRINK MILK \longrightarrow D R I N K @ M I L K

Next, split the chain of letters into groups of the key number. Again, we can use padding with spaces to ensure the last group has enough letters.

DRI NK@ MIL K@@

Now, we use the word shift cipher to encrypt the first group using our keyword. Since we are including spaces, we can just say @ \rightarrow 27. For the second group, we use the word shift cipher again, but now, the keyword is the ciphertext of the first group! Following the pattern, the keyword for the third group is the ciphertext of the second group, and so on.

D	R	I	N	K	@	M	I	L	K	@	@		
4	18	9	14	11	27	13	9	12	11	27	27		
13	15	15	17	6	24	4	17	24	17	26	9		
17	6	24	4	17	24	17	26	9	1	26	9		
Q	F	X	D	Q	X	Q	Z	I	A	Z	I		

\longrightarrow QFXDQXQZIAZI

Exercise:

11. Encrypt the phrase "MADAM I'M ADAM" with the keyword "two" (ignore the apostrophe).
12. Decrypt "ZTDFQYDJELIJ" with the keyword "code"

M	A	D	A	M	@	I	M	@	A	D	A	M	@	@
13	1	4	1	13	27	9	13	27	1	4	1	13	27	27
20	23	15	6	24	19	7	10	19	16	23	19	17	27	20
6	24	19	7	10	19	16	23	19	17	27	20	3	27	20
F	X	S	G	J	S	P	W	S	Q	@	T	C	@	T

\rightarrow FXSGJSPWSQ TC T

W	E	@	A	R	E	@	D	O	N	E	@		
23	5	27	1	18	5	27	4	15	14	5	27		
3	15	4	5	26	20	4	6	17	25	4	10		
26	20	4	6	17	25	4	10	5	12	9	10		
Z	T	D	F	Q	Y	D	J	E	L	I	J		

\longrightarrow WE ARE DONE