SCINNOVA VIII

STUDY GUIDE

CAESAR CIPHER

The Caesar cipher is a code with a numeric key provided. The numeric key identifies how many letters one has to move backwards. For example, the letter F with key +3 would be C.

Decryption

Encrypted text: hqhpb zloo lqlwldwh dq dwwdfn zlwk lqidqwub

1. In this case +3

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
is now
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 key to decrypt the code. In this case, 'enemy will initiate an attack with infantry'

ROT 13

The ROT13 cipher is a substitution cipher with a specific key where the letters of the alphabet are offset 13 places. I.e. all "A"s are replaced with "N"s, all "B"s are replaced with "O"s, and so on. It can also be thought of as a Caesar cipher with a shift of 13.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

NOPQRSTUVWXYZABCDEFGHIJKLM

To decipher a message, find the letter you wish to encipher in the top row, then replace it with the letter in the bottom row. Find the “N” in the top row, which is “A” in the bottom row. Continue until the whole message is done.

Ciphertext: NGGNPX NG QNJA

Plain Text: ATTACK AT DAWN

COLUMNAR CIPHER

The Columnar Cipher is a type of transposition cipher.

Encrypted Text : ethtnmegeotmi

1. If your Keyword is Fancy, it has 5 letters. You would write 31425 because F is the 3rd highest letter in the word and A is the highest letter and so on.
2. Figure out the number of rows using $\frac{Number\ of\ alphabets\ in\ encrypted\ text}{Columns}$

   Note: It’s not necessary that the answer comes out to be a whole number. Specifically in that case, round up and make spaces for only the exact number of extra letters in columns starting from left to right. For example, if we have 3 extra letters and 5 columns, the first three will have one more letter each as compared to the last two columns. An example of this scenario is shown in the diagram below.
3. Start filling in the columns with the encrypted text, starting from the column ranked 1, then 2 and so on.
4. Decrypted text will be visible row-wise.

F	A	N	C	Y
3	1	4	2	5
m	e	e	t	m
e	t	o	n	i
g	h	t		

BINARY TO ASCII

The Binary code is a code that the computers recognize using only 1's and 0's. You will be required to convert the binary code into the corresponding ASCII value to decrypt the text.

0	0011 0000	O	0100 1111	m	0110 1101
1	0011 0001	P	0101 0000	n	0110 1110
2	0011 0010	Q	0101 0001	o	0110 1111
3	0011 0011	R	0101 0010	p	0111 0000
4	0011 0100	S	0101 0011	q	0111 0001
5	0011 0101	T	0101 0100	r	0111 0010
6	0011 0110	U	0101 0101	s	0111 0011
7	0011 0111	V	0101 0110	t	0111 0100
8	0011 1000	W	0101 0111	u	0111 0101
9	0011 1001	X	0101 1000	v	0111 0110
A	0100 0001	Y	0101 1001	w	0111 0111
B	0100 0010	Z	0101 1010	x	0111 1000
C	0100 0011	a	0110 0001	y	0111 1001
D	0100 0100	b	0110 0010	z	0111 1010
E	0100 0101	c	0110 0011	.	0010 1110
F	0100 0110	d	0110 0100	,	0010 0111
G	0100 0111	e	0110 0101	:	0011 1010
H	0100 1000	f	0110 0110	;	0011 1011
I	0100 1001	g	0110 0111	?	0011 1111
J	0100 1010	h	0110 1000	!	0010 0001
K	0100 1011	I	0110 1001	'	0010 1100
L	0100 1100	j	0110 1010	"	0010 0010
M	0100 1101	k	0110 1011	(	0010 1000
N	0100 1110	l	0110 1100	)	0010 1001
				space	0010 0000

MORSE CODE

Morse code is a character encoding scheme used in telecommunication that encodes text characters as standardized sequences of two different signal durations called

dots and dashes or dits and dahs. Following is the table used to decrypt morse code.

Encrypted Text: -- --- .-. ... . -.-. --- -.. .

Decrypted text: Morse code

VIGENERE CIPHER

To decrypt, a table of alphabets can be used, termed a Vigenère table. It has the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the decryption process, the cipher

uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword. One general rule to use the vigenere table is to know where the key column is and where the plaintext row is. The leftmost column is the key column and the top most row is the plaintext row.

For example, suppose that the ciphertext to be decrypted is:

LXFOPVEFRNHR

The person sending the message sends a keyword as well"LEMON". Now to decrypt, you have to repeat it until it matches the length of the plaintext, for example:

LEMONLEMONLE

Each row starts with a key letter. The rest of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, a code will only use as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys: {L, E, M, O, N}. Next go to the row in the table corresponding to the key, finding the position of the ciphertext letter in that row and then using the column's label as the plaintext. For example, in row L (from LEMON), the ciphertext L appears in column A, which is the first plaintext letter. Next, in row E (from LEMON), the ciphertext X is located in column T. Thus, T is the second plaintext letter. The rest of the ciphertext is deciphered in a similar fashion:

CIPHERTEXT:	LXFOPVEFRNHR
KEY:	LEMONLEMONLE
PLAINTEXT:	ATTACKATDAWN

	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

For getting a better understanding of this cIpher please refer to this video:

https://youtu.be/K1SuiUu4kG0

ADFGVX Cipher

To decrypt an ADFGVX Cipher, you use a key and this table:

Table:

\	A	D	F	G	V	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
F	M	N	O	P	Q	R
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

1. If your Keyword is Codes, it has 5 letters. You would write 14235 because C is the highest letter in the word and O is the 4th highest letter and so on.
2. Figure out the number of rows using
   $$\frac{\textit{Number of alphabets in encrypted text}}{\textit{Columns}}$$
   Note: It's not necessary that the answer comes out to be a whole number. Specifically in that case, round up and make spaces for only the exact number of extra letters in columns starting from left to right. For example, if we have 2 extra letters and 5 columns, the first two will have one more letter each as compared to the last three columns. An example of this scenario is shown in the diagram below.
3. Start filling in the columns with the encrypted text, starting from the column ranked 1, then 2 and so on.

Cipher text: AXFAXVDDDDFF

Key: CODES

Table:

C	O	D	E	S
1	4	2	3	5
A	D	A	V	F
X	D	X	D	F
F	D			

You may notice this table in the is how we made our Columnar Cipher.

What's different here is that now you have to read the table from left to right and write down the ciphertext. Next, split the ciphertext into bigrams(2 letters) and read them as coordinates(first letter denotes row, second one denotes column) from the table given at the start. For example:

Ciphertext: ADAVFXDXDFFD

Step 1: AD AV FX DX DF FD

Step 2: B E R L I N

Rail Fence Cipher

Rail Fence Encryption uses an integer key for the number of levels of the zigzag. To decrypt, a zigzag path is formed using the key as the number of rows for the path and number of letters to denote the column, as shown in step 1. Next the ciphertext is written horizontally in all the empty spaces (marked as X), as shown in step 2. Next the text is written along the zigzag path. For example:

Key: 3

Cipher Text : ACTNTAKNIATOY

Step 1: x--------x--------x---------x

--x----x---x----x---x----x

-----x--------x--------x

Step 2: A--------C--------T---------N

--T----A---K----N---I----A

-----T--------O---------T

Decrypted Text: ATTACKONTITAN

Note: This cipher can contain alphanumeric characters and other symbols or a mix of them as well.

Redefence Cipher

Redefence Encryption uses an alphabetic key for the number of levels of the zigzag. The first step is to give an index value to each letter of the key:

Key: ZIG

Cipher Text : TAWTAKTANACD

Step 1: Z (1)

I (2)

G(3)

Next, we arrange those letters alphabetically and write a zigzag pattern as done in rail fence:

Step 2: G(3)x--------x--------x----

I (2)--x----x---x----x---x----x

Z (1)-----x--------x--------x

Next, enter the ciphertext according to the number of rows, the first blanks filled will be the one with index value 1, for example, the letter “TAW” will be filled in row Z because it has index 1 and so on.

Step 3: G (3) A---------C---------D--------

I (2) --T-----A---K-----T---A-----N

Z (1) -----T----------A---------W

To finish up just read the text top to bottom as done in the rail fence cipher. The decrypted text will now be “ ATTACKATDAWN”.

Note: This cipher can contain alphanumeric characters and other symbols or a mix of them as well.

Play fair Cipher

Playfair decryption requires a grid, which can be generated by a keyword. To do so, first you have to use the key provided to make a 5x5 table which has all the letters from A to Z, omitting J, with no repeating values. First you fill in all the characters from the key and ignore any repeating letters. Then fill in the rest of the letters alphabetically. For example:

Key: Playfair

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

Now to decrypt, Split the text into bigrams (two letters) and apply the following rules according to the letter positions in the grid :

- If the 2 letters are on the same row, replace them by the ones on their left (loop to the right if the end of the grid is reached),

Example : PL is decrypted to FP

- If the 2 letters are on the same column, replace them by the ones on their top (loop to the bottom if the end of the grid is reached),

Example : GO is decrypted to RG

- Else, replace the letters by the ones forming a rectangle with the original pair. Beginning with the letter on the same row as the first letter to crypt.

Example : CG is decrypted RK, FU is decrypted PZ.

Note: Delete any unnecessary 'X' if found in the word after decryption.

Four Square Cipher

Four square also requires grids for decryption. But unlike the playfair cipher, it requires four of them which are made using the four keywords provided. To do so, first you have to use the key provided to make a 5x5 table which has all the letters from A to Z, **omitting J**, with no repeating values. First you fill in all the characters from the key and ignore any repeating letters. Then fill in the rest of the letters alphabetically. The sequence of the four keys also denote the grid number, for example:

KEY: BROCK, GEORGE, PAUL, RINGO

Grids:

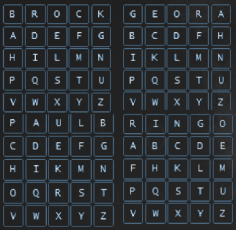
GRID 1: BROCK	GRID 2: GEORGE
GRID 3: PAUL	GRID 4: RINGO

Now, to decrypt the ciphertext you would first break the text in pairs of two. If the number of letters in the ciphertext are odd then add a random letter(**other than J** and the letters used in the ciphertext) to complete the pairs. You will now decrypt the text in pairs. The first letter from pair is located in grid 2 while the second is located in grid 3. Next locate the intersection of the two letters and replace them in the order of grid 1 and then grid 4. For example:

Ciphertext: BPGFIYMX24

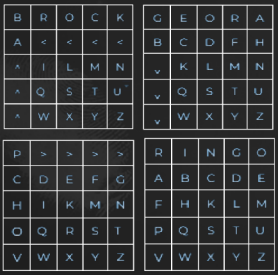
Key: BROCK, GEORGE, PAUL, RINGO

Grids:



Step 1: BP GF IY MX

Step 2: B in grid 2, P in grid 3 leads the intersection to A in grid 1 and R in grid 4. So BP is AR.



Step 3: Repeat step 2 for all bigrams and deciphered text turns out ARCANUM24.

Note: Numeric values stay the same so you just skip over them.

Pigpen Cipher

Pigpen Cipher has its own alphabet of 26 symbols, each corresponding to a letter of the Latin alphabet. To decrypt a message with Pigpen Cipher therefore replace each symbol with the corresponding letter.

Jack Cipher

Jack Cipher has its own alphabet of 26 symbols, each corresponding to a letter of the Latin alphabet. To decrypt a message with Jack Cipher therefore replace each symbol with the corresponding letter.

Code Cipher

Code Cipher has its own alphabet of 26 symbols, each corresponding to a letter of the Latin alphabet. To decrypt a message with Code Cipher therefore replace each symbol with the corresponding letter.

Bean Cipher

Bean Cipher has its own alphabet of 26 symbols, each corresponding to a letter of the Latin alphabet. To decrypt a message with Bean Cipher therefore replace each symbol with the corresponding letter.

Letter	Symbol	Letter	Symbol
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	

NATO PHONETIC ALPHABET

A phonetic alphabet used to spell out letters clearly in communication, especially in noisy or high-stress environments. Each letter of the English alphabet is assigned a distinct word, making it easier to convey and understand the letters, even if the transmission is distorted. Each letter is represented by a word chosen for its clarity and distinctness in pronunciation. Digits 0-9 also have distinct pronunciations to avoid confusion. The words and pronunciations are standardized internationally, ensuring consistent understanding across different languages and accents.

Replace each letter in a message with its NATO Alphabet equivalent.
For example:
Plaintext: HELP
Encoded: Hotel Echo Lima Papa
Below shown are the standard nato alphabets :

HEXADECIMAL

Hexadecimal (base-16) is a numeral system that uses 16 symbols: 0-9 represent values 0 to 9, and A-F represent values 10 to 15. In encoding, each character is converted to its ASCII value, which is then represented in hexadecimal format.

Decoding:
Split hexadecimal values: If the hexadecimal values are concatenated, split them into pairs (1 byte = 2 hex digits).

Convert each hex value to ASCII: Transform each hex value back to its ASCII equivalent.
For example, 48 (hex) becomes H.
Rebuild the original text.

ASCII TABLE

Decimal	Hexadecimal	Char	Decimal	Hexadecimal	Char	Decimal	Hexadecimal	Char
0	0	[NULL]	48	30	0	96	60	`
1	1	[START OF HEADING]	49	31	1	97	61	a
2	2	[START OF TEXT]	50	32	2	98	62	b
3	3	[END OF TEXT]	51	33	3	99	63	c
4	4	[END OF TRANSMISSION]	52	34	4	100	64	d
5	5	[ENQUIRY]	53	35	5	101	65	e
6	6	[ACKNOWLEDGE]	54	36	6	102	66	f
7	7	[BELL]	55	37	7	103	67	g
8	8	[BACKSPACE]	56	38	8	104	68	h
9	9	[HORIZONTAL TAB]	57	39	9	105	69	i
10	A	[LINE FEED]	58	3A	:	106	6A	j
11	B	[VERTICAL TAB]	59	3B	;	107	6B	k
12	C	[FORM FEED]	60	3C	<	108	6C	l
13	D	[CARRIAGE RETURN]	61	3D	=	109	6D	m
14	E	[SHIFT OUT]	62	3E	>	110	6E	n
15	F	[SHIFT IN]	63	3F	?	111	6F	o
16	10	[DATA LINK ESCAPE]	64	40	@	112	70	p
17	11	[DEVICE CONTROL 1]	65	41	A	113	71	q
18	12	[DEVICE CONTROL 2]	66	42	B	114	72	r
19	13	[DEVICE CONTROL 3]	67	43	C	115	73	s
20	14	[DEVICE CONTROL 4]	68	44	D	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	69	45	E	117	75	u
22	16	[SYNCHRONOUS IDLE]	70	46	F	118	76	v
23	17	[ENG OF TRANS. BLOCK]	71	47	G	119	77	w
24	18	[CANCEL]	72	48	H	120	78	x
25	19	[END OF MEDIUM]	73	49	I	121	79	y
26	1A	[SUBSTITUTE]	74	4A	J	122	7A	z
27	1B	[ESCAPE]	75	4B	K	123	7B	{
28	1C	[FILE SEPARATOR]	76	4C	L	124	7C	|
29	1D	[GROUP SEPARATOR]	77	4D	M	125	7D	}
30	1E	[RECORD SEPARATOR]	78	4E	N	126	7E	~
31	1F	[UNIT SEPARATOR]	79	4F	O	127	7F	[DEL]
32	20	[SPACE]	80	50	P			
33	21	!	81	51	Q			
34	22	"	82	52	R			
35	23	#	83	53	S			
36	24	$	84	54	T			
37	25	%	85	55	U			
38	26	&	86	56	V			
39	27	'	87	57	W			
40	28	(	88	58	X			
41	29	)	89	59	Y			
42	2A	*	90	5A	Z			
43	2B	+	91	5B	[			
44	2C	,	92	5C	\			
45	2D	-	93	5D	]			
46	2E	.	94	5E	^			
47	2F	/	95	5F	_			

SPECTROSCOPY

The Principle of Spectroscopy is based on the absorption or emission of light or and radiation by compounds, which results in the production of distinct spectra. Spectroscopy is based on the interaction between light and matter, and depends on the composition of the material. Spectral lines are often used to compare with known spectra and determine a material's composition.

IMAGE STENOGRAPHY

Image steganography is the practice of concealing information within the data of digital images without altering their visual appearance too much. The hidden data can include text, images, audio, or any other form of binary information. It may be in the form of e.g a series of dark and bright pixels encoding in binary or morse code.

The only ciphers used for double encryption are Caesar, Caesar's Box, Atbash, Morse code and Rot 13.

Other than these ciphers used you also need to have a good understanding of the following topics, puzzles and games:

- Minecraft
- Board games
- Phones
- General knowledge of important dates in world history.
- One piece
- Map reading and understanding
- General Mathematical Sequences
- Sherlock Holmes (His mystery solving methods might help you).

SCINNOVA VIII