Grade 7/8 Math Circles
Turing Machines - Problem Set

This problem set will cover a series of activities corresponding to the *Turing Machines* lesson.

Turing Machines

This section provides practice with Turing machines and programs.

1. Use the following instruction table to determine what the output of a blank tape would look like. If the machine runs endlessly, simply determine the output of the first 10 squares. The machine in both part (a) and part (b) will start in state a.

(a)

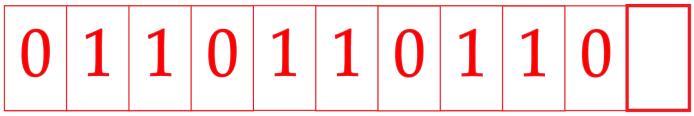
State	Scanned Symbol	Print	Move Tape	Next State
a	blank	0	left	b
b	blank	1	left	c
c	blank	1	left	d
d	blank	0	left	e
e	blank	1	left	stop state

The output of a blank tape after following the above instructions will look like this:

(b)

State	Scanned Symbol	Print	Move Tape	Next State
a	blank	0	left	c
b	blank	1	left	a
c	blank	1	left	b

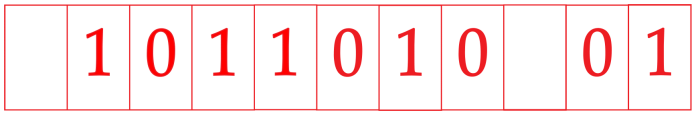
Observe that the machine following the above instructions will run endlessly. So, the output of the first 10 square of a blank tape will look like this:



2. A Turing machine is given a tape with the sequence "10110111". What would be the output of the tape after conducting the following instructions starting from the first 1?

State	Scanned Symbol	Print	Move Tape	Next State
a	blank	0	left	b
	0	1	left	b
	1		left	a
b	blank	1		stop state
	0	1	left	b
	1	0	left	c
c	blank		left	c
	0	1	left	b
	1	1	left	a

The output of the tape after following the above instructions will look like this:



3. It is helpful to construct a state table to summarize how the Turing machine will operate.

   (a) Create a state table for a Turing machine that will repeatedly print the individual digits in 2021.
   This is one possible state table:

State	Scanned Symbol	Print	Move Tape	Next State
a	blank	2	left	b
b	blank	0	left	c
c	blank	2	left	d
d	blank	1	left	a

(b) State tables can help identify an infinite set of instructions from a finite set. Is this program an infinite example or a finite example? Explain how you know.
This is an example of a program running an infinite set of instructions. As we can see from the state table, the machine never enters a stop state and hence, will run continuously.

(c) How must the state table be modified to accomodate a Turing machine that runs a finite set of instructions? Explain.
A Turing machine that runs a finite set of instructions must transition to a stop state at some point. So, the state table must be modified to include a set of instructions where the machine changes to a stop state at the end.

Cracking the Enigma Code

Enigma is the famous cipher machine used by the German military to encrypt messages during World War II. This section will explore some of the mechanics behind the machine.

4. An Enigma machine utilizes a straightforward method of encoding messages called *substitution encryption*. The simplest example of such a cipher is the *Caesar cipher* produced by shifting the alphabet some units to the right. Originally used by Roman general Julius Caesar, the original Caesar cipher was created by shifting the alphabet three letters to the right, as shown below.

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

(a) Use the original Caesar cipher to encrypt the following message: "TURING MACHINES ARE COOL".

Using the original Caesar cipher, we get

T → V	M → O	A → C	C → E
U → W	A → C	R → T	O → Q
R → T	C → E	E → G	O → Q
I → K	H → J		L → N
N → P	I → K		
G → I	N → P		
	E → G		
	S → U		

So, the encoded message would be "VWTKPI OCEJKPGU CTG EQQN".

(b) Fill in the table for a Caesar cipher with a shift of 5. Use this cipher to encode the message from part (a).

A	B	C	D	E	F	G	H	I	J	K	L	M
E	F	G	H	I	J	K	L	M	N	O	P	Q

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D

Now, using this new Caesar cipher, we get

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

So, the message from part (a) would now be encoded as "XYVMRK QEGLMRIW EVI GSSP".

(c) Use a Caesar cipher with a shift of -1 to encode your name. (*Hint:* Try creating a table like the ones above if you need help)

Individual answers will vary.

Enigma machines are made up of several parts: a keyboard, a lamp board, rotors, a plugboard, and internal electronic circuitry. This leads their encryption to be much more complex than a simple Caesar cipher.

5. First, there would be a set of plugboard settings. A plugboard would have 26 slots, one for each letter of the alphabet, and wires with two ends could plugged into these slots. So, each plug wire can connect two letters to be a pair and these letters would swap over. For example, if "A" is connected to "Z", "A" would become "Z" and "Z". Using this rule, the word "ZEBRA" would be encoded as "AEBRZ". Combining it with more levels of substitution encryption, our simple Caesar cipher with a shift of 3 would now look like this:

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

   (a) If the plugboard connects the letters E and S, what would the word "MESSAGE" be encoded as?
   The word "MESSAGE" would be encoded as "MSEEAGS".

   (b) The plugboard on an Enigma machine would typically use 5 separate wires to create 5 pairs of letters that would switch. If the plugboard settings connected the letters A & L, P & R, T & D, B & W, and K & F, then what would the following message be encoded?
   original message: "AN APPLE A DAY KEEPS THE DOCTOR AWAY"
   encoded message: "LN LRRAE L TLY FEERS DHE TOCDOP LBLY"
   First, replace all the As with Ls and vice versa: "LN LPPAE L DLY KEEPS THE DOCTOR LWLY"
   Then, replace all the Ps with Rs and vice versa: "LN LRRAE L DLY KEERS THE DOCTOP LWLY"
   Next, replace all the Ts with Ds and vice versa: "LN LRRAE L TLY KEERS DHE TOCDOP LWLY"
   Now, replace the W with a B: "LN LRRAE L TLY KEERS DHE TOCDOP

LBLY"

Finally, replace the K with an F: "LN LRRAE L TLY FEERS DHE TOCDOP LBLY"

6. Then, the machines used three rotors at a time to encode a message. Each rotor provided a different encoding scheme. So, if the initial position of the alphabet looks like:

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

Here's how it would look after the first turn:

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

Here's how it would look after the second turn:

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

Here's how it would look after the third turn:

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

For example, if the word "PEN" went through the rotors above, the resulting encoded word would be "CEB".

(a) Consider if the message "ROTARY CHICKEN" went through the rotors. What

would be the encoded message?

Using the encoding scheme, we get

$$\begin{array}{ll} R \to X & C \to J \\ O \to R & H \to D \\ T \to K & C \to J \\ A \to S & I \to H \\ R \to X & K \to Z \\ Y \to I & E \to E \\ & N \to B \end{array}$$

Hence, the encoded message would be "XRKSXI JDHJZEB".

(b) Steven writes the message "DSCCI MCXHBN VXESZ" using the alphabet legend for the encoding scheme after the third turn. What was his original message? If he uses another set of three rotors to change up the encoding scheme, what would be the new message?

If we use the alphabet legend, we can decrypt Steven's message. So,

$$\begin{array}{lll} D \to H & M \to S & V \to B \\ S \to A & C \to P & X \to R \\ C \to P & X \to R & E \to E \\ C \to P & H \to I & S \to A \\ I \to Y & B \to N & Z \to K \\ & N \to G & \end{array}$$

Therefore, his original message was "HAPPY SPRING BREAK". If he uses another set of three rotors to change up the encoding scheme, the alphabet legend will look like this after the first turn:

A	B	C	D	E	F	G	H	I	J	K	L	M
L	S	V	J	G	E	T	N	D	H	Q	Z	U

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

Here's how it would look after the second turn:

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

Here's how it would look after the third turn:

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

Now using this encoding scheme to encrypt his original message, we get

$$\begin{array}{lll} H \to E & S \to C & B \to I \\ A \to F & P \to P & R \to R \\ P \to P & R \to R & E \to V \\ P \to P & I \to T & A \to F \\ Y \to A & N \to Z & K \to D \\ & G \to G & \end{array}$$

Therefore, the new encoded message is "EFPPA CPRTZG IRVFD".

(c) Take the message from question 5.(b). What would be the original message after it has gone through the above encoding scheme? What would the encoded message be after it goes through the encoding scheme?

If we take the original message from question 5.(b), "AN APPLE A DAY KEEPS THE DOCTOR AWAY", and apply the encoding scheme, then we get

$$\begin{array}{llllllll} A \to S & A \to S & A \to S & K \to Z & T \to K & D \to G & A \to S \\ N \to B & P \to C & & E \to E & H \to D & O \to R & W \to W \\ & P \to C & D \to G & E \to E & E \to E & C \to J & A \to S \\ & L \to U & A \to S & P \to C & & T \to K & Y \to I \\ & E \to E & Y \to I & S \to M & & O \to R & \\ & & & & & R \to X & \end{array}$$

So, the original message from 5. (b) is encoded as "SB SCCUE S GSI ZEECM KDE GRJKRX SWSI". Now, we take the encoded message from question 5. (b),

"LN LRRAE L TLY FEERS EHE TOCDOP LBLY", and apply the encoding scheme. Then, we get

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

Therefore, the encroded message from question 5. (b) is encrypted as "UB UXXSE U GUI TEEXM GDE KRJGRC UVUI.".