NAME: ELENDU CHIDERA ISABELLA

DEPT: COMPUTER ENGINEERING

MATRIC NO: 15/ENG02/021

ASSIGNMENT

QUESTION 1: Write notes on autokey cipher and discuss computer crimes.

ANSWER

Autokey Cipher

An autokey cipher is a cipher which integrates a plain text into a keystream. It was first described by Girolamo Cardano and consisted of the plain text itself as the keystream. The most famous version of the Autokey Cipher was described by Blaise de Vigenere in 1586.

There are two forms of autokey cipher: key autokey and text autokey. A key autokey cipher uses previous members of the keystream to determine the next element in the keystream. Whereas, a text autokey uses the previous message to determine the next element in the key stream.

One popular form of Autokey starts with a **tabula recta;** this is a square which contains 26 copies of the English Alphabet, the first line starts with an "A" and the next line with a "B". So, to encrypt a plain text, the row with the first letter and the column with the first letter of the key are being chosen (highlighted). The letter where the row and column cross is the cipher text letter.

For example; if a **plaintext** is given; **Send my dagger**, and a **keyword**; **John**. The first thing that should be done is generate the keystream. This is done by combining the keyword and plaintext together; the keyword first, then the plain text follows.

Hence, plain text:	s	e	n	d	m	y	d	a	g	g	e	r				
Keystream:	j	o	h	n	s	e	n	d	m	y	d	a	g	g	e	r

Next, the Tabula Recta is used to find the cipher text.

The result,

Plain text:	s	e	n	d	m	y	d	a	g	g	e	r				
Keystream:	j	o	h	n	s	e	n	d	m	y	d	a	g	g	e	r
Cipher text:	b	r	u	q	e	c	q	d	s	e	h	r				

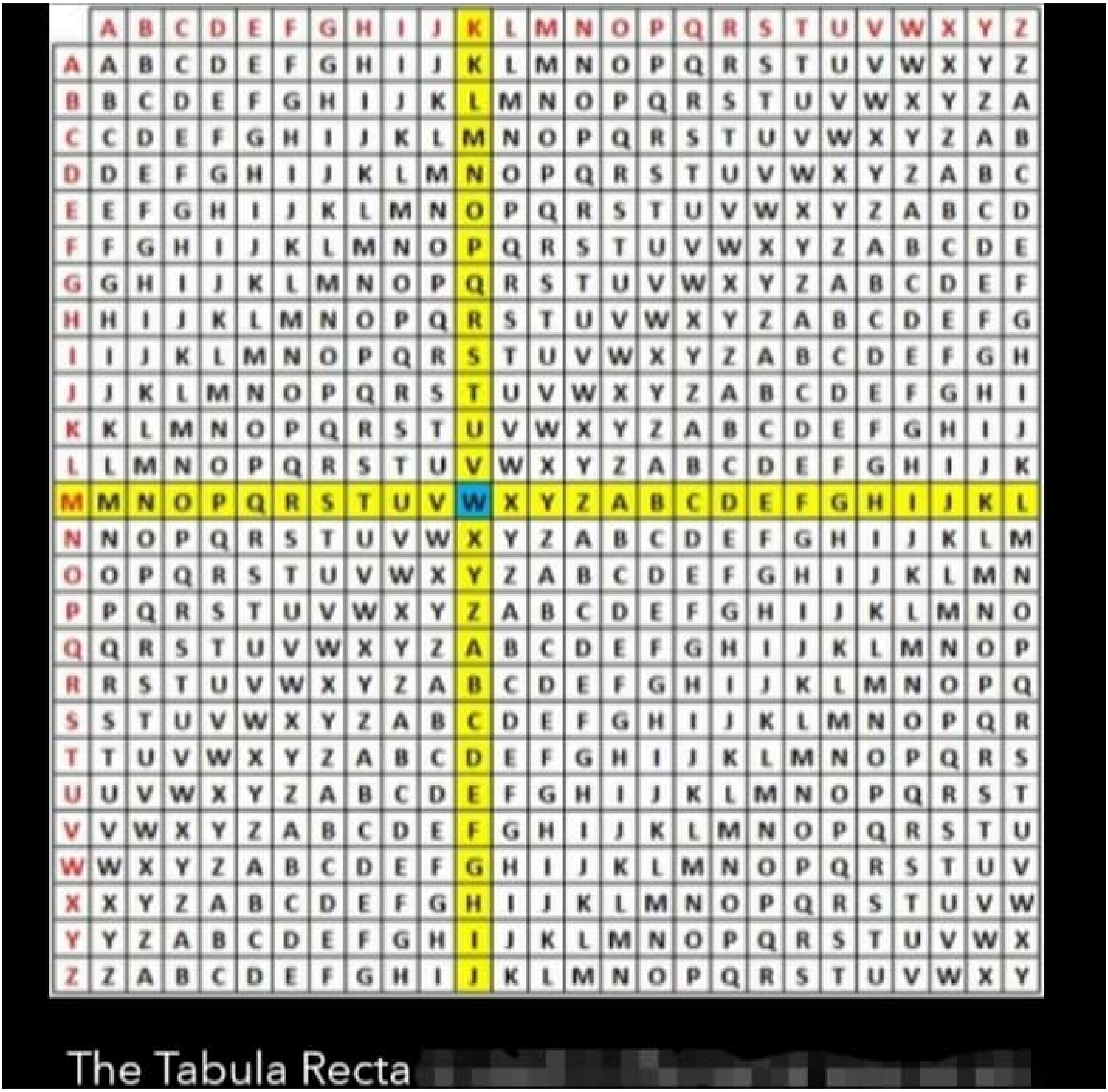
To decrypt a ciphertext using the autokey cipher, we find the first letter of the key across the top , find the cipher text down the column and take the plaintext letter at the far left of the row. Next, the letter will then be added to the end of the keystream. Decoding continues and it is added to the end of the keystream after every step.

Computer Crimes

A **Computer crime** is an act performed by a computer literate. It is the use of a computer (and the internet) as a tool to operate illegally, Examples of these computer crimes include; stealing identities, violating privacies, child pornography, etc. These are specific crimes with specific victims, but the criminal hides (remains anonymous) using tools provided by the internet.

Another part of this computer crime involves individuals within corporations deliberately using data for profit or political objectives. These include; denial of service attacks, spam attacks, etc.

All these could cause public disturbances and even death to individuals (cyber bullying).



	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

The Tabula Recta [redacted]