Code Busters Practice Test

You have 45 Minutes to complete this test

Record your time when you finish the first question

For added realistic test conditions, have someone else know the answer to the first question and tell you if you are correct or incorrect. If incorrect, you may try again. Record the time when you get the question correct.

For the purposes of this test, A=0,B=1,C=2… Z=25

For mono-alphabetic substitution cyphers the only constraint on ciphertext alphabets is that no letter may decrypt to itself

You may need the following 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

Question 1

Worth 400pts + Timing Bonus

Timing bonus = 4 * (600 – time(s))

The following cipher is a mono-alphabetic substitution with spaces

JGQW SBE GMS YHWG JBF AEVJ PSOGMPD IWGO PJW NWBNLW PJWS BNOWDD? GLL BI PJWA OWGLYTW PJGP, BMW HGS, GABMXDP PJWYO AGMS QYVPYAD, PJWOW YD DEOW PB BMW PJGP OYDWD GXGYMDP PJWA GMH DPOYZWD UGVZ!

	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
freq	6	9	0	12	3	1	16	3	2	11	0	4	8	3	9	17	2	0	6	1	1	3	20	2	9	2
	G	U	V	H	W	I	X	J	Y	K	Z	L	A	M	B	N	C	O	D	P	E	Q	F	R	S	T

Have you any idea how much tyrants fear the people they oppress? All of them realize that, one day, amongst their many victims, there is sure to be one that rises against them and strikes back!

Question 2

Worth 200 pts

The following ciphertext is a mono-alphabetic substitution from Jean Jacques Rousseau's *Social Contract*. One thing to note is that Rousseau likes to use masculine pronouns

XLY TD MZCY QCPP, LYO PJPCJHSPCP SP UD TY NSLTYD. SPCP'D ZYP HSZ ESTYVD SP UD DSP XLDEPC ZQ ZESPCH, JPE SP UD XZCP PYDWLGPO ESLY ESPJ LCP.

	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
freq	0	0	9	10	6	0	1	3	0	4	0	7	1	1	2	21	2	0	12	4	3	1	1	3	9	6
	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

Man is born free, and everywhere he is in chains. Here's one who thinks he is the master of others, yet he is more enslaved than they are.

Question 3

Worth 400 pts

The following cipher text encoded using a mono-alphabetic substitution is from the last 2 sentences in the book Don Quixote. It is written in the past tense. The plain text is in the original language: Spanish. Accents are ignored. This cipher uses a 27-letter alphabet, Ñ is considered its own letter while CH, LL are considered 2 each.

HNGAÑIYRN, YRPOÑ, AN JY ÑZZYUPÑI TVN FN LN AYAÑ AN HYGNZNG JÑZÑ ZÑRÑ XÑ LYZPNIAÑFN ZYNG NI NJ NGGÑG NI TVN XÑ ZYPAÑ AN TVN LVBÑ X LYX ZYBYJJNGO YIAYIFNU NI NJ RVIAÑ.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
freq	10	2	0	0	0	3	8	2	9	6	0	4	0	23	16	2	4	0	4	0	3	2	5	0	4	14	9
	Y	B	Z	A	N	M	O	L	P	K	Q	J	R	I	S	Ñ	H	T	G	U	F	V	E	D	W	X	C

Perdoname, amigo, de la occasion que te he dado de parecer loco como yo haciendote caer en el error en que yo he caido de que hubo y hay caballeros andantes en el mundo.

Question 4

Worth 500 pts

No hint for this one

CX CO I NSFCEJ EB ACPCD YIF. FSRSD ONIASOTCNO, OXFCUCMB BFEV I TCJJSM RIOS, TIPS YEM XTSCF BCFOX PCAXEFQ IKICMOX XTS SPCD KIDIAXCA SVNCFS

	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
freq	5	4	16	4	5	9	0	0	10	3	2	0	2	4	8	4	1	2	12	5	1	4	0	8	2	0
	I	R	A	J	S	B	K	T	C	L	U	D	V	M	E	N	W	F	O	X	G	P	Y	H	Q	Z

It is a period of civil war. Rebel spaceships, striking from a hidden base, have won their first victory against the evil Galactic Empire.

Question 5

Worth 600 pts

The following ciphertext is a mono-alphabetic substitution with typos.

HVS ACIFBWU VOR RKBR QZSSF OBR QCZR, KWHV O QFWGDBSGG HVOH VBHSR OH HVS OBR CT GIAASF. HVOM GSH TCFHV OH RSMPFOY HC GSS O AOB PSVSRSR, HKSBHSS WB OZZ, ZBR PFOB FCRS OACIBU HVSA, BSFJIG KWHV SLGWHASBH

	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
freq	7	14	7	1	0	9	8	18	4	1	4	1	2	0	14	3	3	12	22	2	2	11	6	0	1	5
	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

The mourning had dwnd cleer and cold, with a crispness that hnted at the and of summer. Thay set forth at deybrak to see a man beheded, twentee in all, and Bran rode among them, nervus with exsitment.

Question 6

Worth 550 pts

The following ciphertext is taken from *The Hobbit* by J.R.R. Tolkien. The word “in” appears 3 times, the word “hobbit” appears twice, and the word “hole” appears 4 times. Spaces and punctuation have been removed.

YTGZ SVCY TNZC QPWM TDNZ CPCV YLCD GZSF FYNT SNGT GONI DYPN IKCN ZSVC BYVV CDKY NZNZ CCTD OSBK SPUO GTDGT SSHI OUCVV TSPI CNGD PIFG PCOG TDIZ SVCK YNZT SNZY TAYT YNNS OYND SKTS TOPN SCGN YNKG OGZS FFYN ZSVC GTDN ZGNU CGTO ESUB SPN

	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
freq	1	3	17	10	1	5	15	1	6	0	6	1	1	22	9	9	1	0	19	17	4	9	1	0	14	13
	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H

In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort.

Question 7

Worth 700 pts

No clue, no punctuation, no spaces.

CJRN OPKD YJAH ZWPO DQZI ZQZM NZZI VNJI JAVY VHJM VYVP BCOZ MJAZ QZWZ AJMZ

	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
freq	4	1	2	2	0	0	0	2	3	7	1	0	4	3	3	3	3	1	0	0	0	5	2	0	3	11
	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

How stupid of me! But I’ve never seen a Son of Adam or a Daughter of Eve before.

Question 8

Worth 300 pts

Encode the following sentence using an affine cipher with a key of 5x+4

SPACE, THE FINAL FRONTEIR. THESE ARE THE VOYAGES OF THE STARSHIP ENTERPRISE.

	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
Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
5x	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125
5x + 4	4	9	14	19	24	29	34	39	44	49	54	59	64	69	74	79	84	89	04	99	104	109	114	119	124	129
Ans mod 26	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0	5	10	15	20	25
	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z

QBEOY, VNY DSREH DLWRVYSL. VNYQY ELY VNY FWYEIYQ WD VNY QVELQNSB YRVYLBLSQY.

Question 9

Worth 600 pts

This affine ciphertext is encoded from a cryptography textbook. It is the first 2 sentences from the first chapter on modular arithmetic. The word modular occurs once and the prefix crypto occurs twice. The key is ax + b. Decrypt the message or determine the key

XBFO LA UOVN YLLJ PVQQ YT NSTEU QLLJVRH RU UOT RSSQVFRUVLEN LA XLMBQRG RGVUOXTHVF, NVEFT VU VN ABEMRXTEBRQ UL XLMTGR FGDSULHGRSOD REM SBUQVF JTD FGDSULNDNUTXN VE SRGUVFBQRG. OTEFT, VE UOVN FORSUTG PT VEUGLMBFT UOT YRNVF FLEFTSUN REM UTFOEVZBTN PT NORQQ GTZBVGT

	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
Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
freq	3	9	0	5	13	15	12	3	0	3	0	14	6	13	11	3	10	17	10	21	19	19	0	6	3	2

Much of this book will be spent looking at the applications of modular arithmetic, since it is fundamental to modern cryptography and public key cryptosystems in particular. Hence, in this chapter we introduce the basic concepts and techniques we shall require.

7x+17

Question 10

Worth 500 points

The Dread Pirate Roberts needs your help encrypting this phrase. He started from the end and needs your help finishing. Finish encrypting the following phrase using a hill cipher with a key of ASYOUWISH. The strikethrough has already been encrypted, only encrypt the bold

HELLO, MY NAME I~~S INIGO MONTOYA. YOU KILLED MY FATHER. PREPARE TO DIE~~

______, __ _____ __ ______ ________. __I YGINCM VS OFRMLN. MVMSTFC EE GVO

	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
Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

YJXUP, IA EKEY Q

Question 11

Worth 600 pts

Find the decryption key for a hill cipher with a key of HOLYGRAIL with this 29 letter 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	;	|	+
Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

$$\begin{pmatrix} H & O & L \\ Y & G & R \\ A & I & L \end{pmatrix} = \begin{pmatrix} 7 & 14 & 11 \\ 24 & 6 & 17 \\ 0 & 8 & 11 \end{pmatrix}$$

$$\begin{vmatrix} 7 & 14 & 11 \\ 24 & 6 & 17 \\ 0 & 8 & 11 \end{vmatrix} = 7\begin{vmatrix} 6 & 17 \\ 8 & 11 \end{vmatrix} - 14\begin{vmatrix} 24 & 17 \\ 0 & 11 \end{vmatrix} + 11\begin{vmatrix} 24 & 6 \\ 0 & 8 \end{vmatrix}$$

$$= 7(6*11 - 17*8) - 14(24*11-0*17) + 11(24*8-0*6) = -2074$$

$-2076\ mod\ 29 = 12;$ $\qquad 12*x = 1\ mod\ 29 \qquad x=17$

$$adj\begin{pmatrix} 7 & 14 & 11 \\ 24 & 6 & 17 \\ 0 & 8 & 11 \end{pmatrix} = \begin{pmatrix} +\begin{vmatrix} 6 & 17 \\ 8 & 11 \end{vmatrix} & -\begin{vmatrix} 14 & 11 \\ 8 & 11 \end{vmatrix} & +\begin{vmatrix} 14 & 11 \\ 6 & 17 \end{vmatrix} \\ -\begin{vmatrix} 24 & 17 \\ 0 & 11 \end{vmatrix} & +\begin{vmatrix} 7 & 11 \\ 0 & 11 \end{vmatrix} & -\begin{vmatrix} 7 & 11 \\ 24 & 17 \end{vmatrix} \\ +\begin{vmatrix} 14 & 11 \\ 6 & 17 \end{vmatrix} & -\begin{vmatrix} 7 & 11 \\ 24 & 17 \end{vmatrix} & +\begin{vmatrix} 7 & 14 \\ 24 & 6 \end{vmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} -70 & -66 & 172 \\ -264 & 77 & 145 \\ -72 & -145 & 294 \end{pmatrix} = \begin{pmatrix} 17 & 21 & 27 \\ 3 & 19 & 0 \\ 15 & 0 & 4 \end{pmatrix} \quad mod\ 29$$

$$17 * \begin{pmatrix} 17 & 21 & 27 \\ 3 & 19 & 0 \\ 15 & 0 & 4 \end{pmatrix} = \boxed{\begin{pmatrix} 28 & 9 & 24 \\ 25 & 20 & 0 \\ 23 & 0 & 10 \end{pmatrix}}$$

Question 12

300 pts

Encode the following plain text using a Vigenère Cipher with a key of BUTTERCUP

LIFE IS PAIN, HIGHNESS.

MCZY MJ RUYO, BNGLHGOH.

Question 13

300 pts

Decrypt this Baconian cipher with a 24 letter alphabet (I,J and U,V are one letter)

ABABBABAAABABABAABAA ABABBABBBAABBABAABBA AAAAAABBABAAABB ABBBBBAAABABBBABAABAABBBBAABAABAAAB

Live long and prosper

Question 14

500 points

Encrypt the following with a running key cipher using this test booklet as the key. Ignore all special characters and numbers. Ignore ciphertext and tables.

A ROBOT MAY NOT INJURE A HUMAH BEING OR THROUGH INACTION ALLOW A HUMAN BEING TO COME TO HARM

CFRFPNETCEGIZNLNZGEAYETHOCYHKGKBVEGNUDWYFENSWRRRXOELJIYYBVLII
KFWPIFILHVCFY

Question 15a

400 points

Given prime numbers p =79 and q = 83 and exponent e=5, generate the RSA public and smallest possible private key.

79 * 83 = 6557

Public key (6557, 5) 200 pts

Theta(n) = 78*82 = 6396

(4 Theta(n)+1)/5 = 5117

Private Key = 5117 200 pts

Question 15b

200 points

Using the keys above, encrypt the number 81

$81^5 \bmod 6557 = 1296$

Question 15c

100 pts

Mathematically set up how to decrypt the ciphertext 2345 using the above key

2345^ 5117 mod 6557

Question 16

450 pts

Crack this Vigenère cipher given the following plain text:

THE BOY WHO LIVED

And the following ciphertext:

IHXSCLQZDLBMSQ

PATRONUS