last name ______________________________ *ID* ______________________________

c/cmaker/cbreaker 2012 exam version a

6 pages 3 hours 40 marks no electronic devices **SHOW ALL WORK**

8	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
1	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
3	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
4	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
12	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
2	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
2	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
6	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
7	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
0	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
1	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
4	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
2	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
7	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
8	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
2	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
0	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
6	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
6	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
9	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
3	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
1	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
2	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
0	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
2	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
0	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

x * y (mod 23)

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

$\alpha\;\beta\;\chi\;\delta\;\epsilon\;\phi\;\gamma\;\theta\;\iota\;-\;\kappa\;\lambda\;\mu\;\nu\;o\;\pi\;-\;\rho\;\sigma\;\tau\;\upsilon\;-\;\omega\;\xi\;-\;\zeta$

1. [8 marks] Assume Caesar spoke English. Encrypt *we come to rescue* as he did when he found his troops surrounded by Gauls.

Assume Caesar spoke English. Encrypt *i will be emperor* as he would write in his diary.

Which of these is the most likely plaintext for 1-time pad ciphertext *iyxtybppzmewza*? Why?

`firemissilenow`

`retreatatdawnx`

`sixhundredcash`

Encrypt *lose weight fast* with the ADFGVX cipher. Use the grid below and keyword *trap*.

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

2. [4 marks] `sp oyh kyxf iyfl oyh nzil xy dsgnf fy rywavzsx`

   According to Al Kindi, what are the first two substitutions you should try on this ciphertext?

   One plaintext word is *vote*. Break the cipher.

3. [4 marks] Using Vigenere with key `grave`, encrypt *two can keep a secret if one is dead.*

   Here are Vigenere ciphertext repeated 3-gram offsets: `dtt 49 btd 147 tgf 91 mde 43 qpz 133`.
   What is the likely keylength? Why? Are any of these a false positive?

4. [6 marks] Align `wettervorhersagere` to start at the first possible position in the following Enigma ciphertext. Draw the Turing graph. List all cycles.

   `... G S R P Q N H R W X R H I X S F U L E P P P ...`

   Describe the components of the Enigma (at the start of the war). Use this information to estimate the number of different keys.

   What do Rejewski's method and Turing's method have in common that allows their success?

5. [2 marks] Draw an evolutionary diagram including these ciphers: running key, RSA, polybius, 1-time pad, homophonic, substitution, Caesar, Vigenere, ADFGVX. (In the diagram, draw an arrow from A to B if B evolved from A.)

6. [5 marks] DHM was created to solve what cryptographic problem ? (at most 10 words)

Alice and Bob use DHM with $n = 23$ and $b = 5$. Alice sends Bob 11. Bob sends Alice 10.

You are Eve. Find Bob's secret number (see page 1) ...

...and find the number Alice and Bob create together.

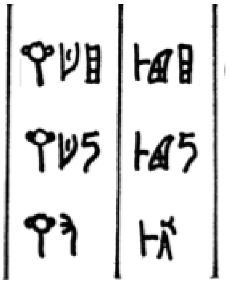
7. [3 marks] Alice's RSA values are $n = 2021$ and $e = 671$. Bob encrypts his message (the number 877) with this system. Give a mathematical expression that equals the number Bob sends Alice.

You are Eve. $2021 = 43 * 47$. Find Alice's secret number d. The equations below might help.

```
590 - 81 * 7 = 23
81 - 23 * 3 = 12
23 - 12 * 1 = 11
12 - 11 * 1 = 1

1  =  12 * 1  +  11 * -1
1  =  23 * -1  +  12 * 2
1  =  81 * 2  +  23 * -7
1  =  590 * -7  +  81 * 51
```

8. [4 marks]



The table at left corresponds to the table at right (symbol ↔ number). For each symbol pair below, what if anything do the two symbols have in common, and why?

0 1 2	5 6 2
0 1 3	5 6 3
0 4	5 9

(1,4)

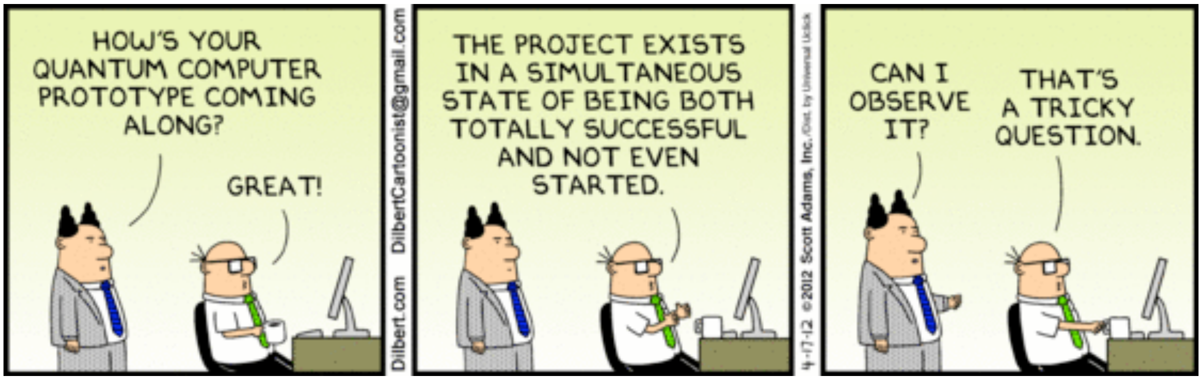
(1,6)

(2,3)

What crib helped break this language?

9. [4 marks] Why is panel 1 funny?

Why is panel 3 funny?


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Dilbert.com DilbertCartoonist@gmail.com

4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick