c/cmaker/cbreaker 2013 exam no electronic devices version b

6 pages + refpage 3 hours 50 marks **all plaintext is English show all work**

1. [1.5 + 1.5 + 1.5 + 1.5 marks]

(i) Thomas Phelippes is best known for

_ _

in the year _ _ _ _ _ _ _ _ _ _ _ _ _.

(ii) In the year _ _ _ _ _ _ _ _, Alberti built a _ _ _ _ _ _ _ _ _ and described a _ cipher.

(iii) In the context of evolution, (i) and (ii) might seem surprising, because

_ _.

_ _.

(iv) After further thought, it is not so surprising, because

_ _.

_ _.

2. [1.5 + 1.5 marks]

ςιπηερσ αρε βροκεν σομετιμεσ

According to historian _ _ _ _ _ _ _ _ _ _ _, _ _ _ _ _ _ _ _ _ _ _ _ used a cipher like this around the year _ _ _ _ _ _ _ _ _ _ _ _ _.

Break the cipher. Explain briefly.

3. [1 + 2 + 1 + 4 marks]

```
 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
length 1
 1  0  0  2  3  4  0  3  0  0  3  3  1  0  0  0  2  0  1  2  3  3  2  0  0  1 34 0.0485
length 2
 1  0  0  0  2  3  0  3  0  0  1  1  0  0  0  0  1  0  0  1  1  1  2  0  0  0 17 0.0556
 0  0  0  2  1  1  0  0  0  0  2  2  1  0  0  0  1  0  1  1  2  2  0  0  0  1 17 0.0347
length 3
 0  0  0  1  1  0  0  3  0  0  1  0  0  0  0  0  0  0  0  0  1  3  1  0  0  1 12 0.0839
 0  0  0  0  2  0  0  0  0  0  0  3  0  0  0  0  0  0  1  2  2  0  1  0  0  0 11 0.1
 1  0  0  1  0  4  0  0  0  0  2  0  1  0  0  0  2  0  0  0  0  0  0  0  0  0 11 0.133
length 4
 0  0  0  0  0  3  0  1  0  0  0  1  0  0  0  0  0  0  0  1  0  1  2  0  0  0 9 0.1
 0  0  0  0  0  1  0  0  0  0  2  2  0  0  0  0  1  0  1  0  1  1  0  0  0  0 9 0.05
 1  0  0  0  2  0  0  2  0  0  1  0  0  0  0  0  1  0  0  0  1  0  0  0  0  0 8 0.0635
 0  0  0  2  1  0  0  0  0  0  0  0  1  0  0  0  0  0  0  1  1  1  0  0  0  1 8 0.0317
```

(i) Assume this is a substitution cipher. Show the first Al Kindi substitution:

`vlazlk euf vudhlk, vwqht fuemws qdt fhefk`

`------ --- ------  ----- ------ --- -----`

(ii) This is probably not a Kama Sutra cipher, which is a kind of _ _ _ _ _ _ _ _ _ _ cipher, because those ciphers have _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ of about _ _ _ _ _ _ _, whereas here this value is about _ _ _ _ _ _ _.

(iii) This is probably a _ _ _ _ _ _ _ _ _ cipher with keyword length _ _ _ _ _ _.

(iv) Break the cipher. Explain briefly.

`vlazlk euf vudhlk, vwqht fuemws qdt fhefk`

`------ --- ------  ----- ------ --- -----`

4. [2 + 2 + 2 + 2 marks]

In year _ _ _ _ _ _ in country _ _ _ _ _ _ _ _,

_ _ _ _ _ _ _ _ _ _ first broke the Enigma, by exploiting this German protocol: _.

The number of different keys at this time was around 10 to the power _ _ _ _ _, but his lookup table — indexed by _ _ _ _ _ _ _ _ _ _ _ _ _ _ — needed only about _ _ _ _ _ _ _ _ entries, because this was the number of _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _.

Align `wettervorhersagere` at the first possible position:

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

For this alignment, draw the Turing graph. List all cycles.

5. [3 marks]

In year _ _ _ _ _ _ Zimmerman created the encryption system

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _, which upset two groups of people:

_ _ _ _ _ _ _ _ _, because _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _;

_ _ _ _ _ _ _ _ _, because _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _.

6. [$2 + 2 + 1$ marks]

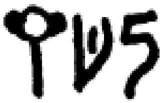
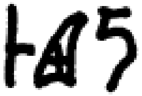
The inverse of 31 mod t is the integer k, such that _ _ _ _ _ _ is equal to _ _ _ _ _ _ plus some integer times _ _ _ _ _. $\phi(n)$ is the number of integers in $\{1, 2, \ldots, n\}$ that _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _.

Alice uses RSA and publishes $n = 2501$ and $e = 821$. You are Eve. You know that Alice's favorite number is 61. Fill in the blanks.

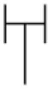
```
___ - ___ * 2 = 758

821 - 758 * 1 = 63

758 - 63 * 12 = 2

63 - 2 * 31 = 1

1  =  63 * 1  +  2 * -31

1  =  758 * -31  +  63 * 373

1  =  821 * 373  +  758 * -404

1  =  ____ * -404  +  821 * ____
```

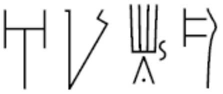
You intercept the number 1943 that Bob sends Alice. An arithmetic expression for m, Bob's secret message to Alice, is _ _ _ _ _ _ _ _.

7. [4 + 2 + 3 marks]

Looking at  and , _ _ _ _ _ _ _ _ _ _ _ _ guessed that symbols _ _ _ _ _ _ _ _ and _ _ _ _ _ _ _ _ have this property:

_ _.

Continuing her work, _ _ _ _ _ _ _ _ _ _ _ _ _ guessed  is a _ _ _ _ _ _ _.

Later, he deduced that  is the word for _ _ _ _ _ _ _ _ _ _ _ _.

Encrypt *desperate* with the ADFGVX cipher. Use grid and keyword *prat*.

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

This cipher evolved from the _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _, described around 150BC for telegraphy. The cipher was broken in year _ _ _ _ _ _ _ in country _ _ _ _ _ _ _ _ _ by _ _ _ _ _ _ _ _. Around this time Morse fists were used to identify battle groups that sent messages by _ _ _ _ _ _ _ _, by a process known as _ _ _ _ _ _ _ _ _.

8. [3 + 1 marks]

(i) These two one-time pad ciphertexts were generated with the same key. The first plaintext starts “`attack...`”. Find the two plaintexts.

```
u e z s v e d m u u l x c z

_ _ _ _ _ _ _ _ _ _ _ _ _ _

n l q w g i n m o a o g b x

_ _ _ _ _ _ _ _ _ _ _ _ _ _
```

(ii) The method used in (i) is similar to the method used to break a

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _.

9. [4 marks]

Alice and Bob use the _ _ _ _ _ _/Bratley protocol: 0/1 for rect/diag filters, 0/1 for `-/+` particle polarisation, 0/1 for `\//` particle polarisation. Alice uses the random sequences _ _ _ _ _ _ _ _ _ _ _ _ for filter selection and 0101 1011 0111 for key construction, and sends Bob the particle sequence `-/\+ /-+/ \/+/` Bob uses 1010 1011 1001 for filter selection, and detects this sequence as `??01` _ _ _ _ _ _ _ _. On an insecure line, Alice and Bob tell each other their filter sequences. The key they have created so far is _ _ _ _ _ _ _ _ _ _ _ _ _ _. For eavesdropping detection, Alice tells Bob that the first two bits are `01`, and Bob tells Alice that he agrees, so the probability that Eve was intercepting the particle channel is at most _ _ _ _ _.

reference material

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