Codebusters C
Exam

University of Chicago Science Olympiad Invitational 2019

Saturday, January 12, 2019

Instructions:

0. **Wait** until told to open the test.

1. For Affine, Hill (State level), and RSA (State level) questions, use ‘a’ = 0, ‘b’ = 1, ... rather than starting with ‘a’ = 1.

2. Don’t worry too much about the State-level questions if you can’t get them. They’re mainly there for fun and as an extra challenge -- but still give them a try!

3. Grading mostly follows the rules (≤ 2 mistakes is full score; you lose 100 points for every mistake past that). But the timing bonus will be scaled down by a factor of 4 (600 points max).

Regional-level questions [3200 pts + time bonus]

1. Timed Aristocrats w/ Hint [500 pts + 600 time bonus (scaled down by 4)]:

Ciphertext:

Jrv esllsov tzwcl crvdv sj sl pj poo jsevl.

Sj tzwcl jrsl hvgpklv sj tzwcl crvd

v sj slzj, hi lkhjdpgjszu crvdv sj sl qdwe

crvdv sj slzj, wd crvdv sj slzj qd

we crvdv sj sl, sj whjpszl p msqqvdvzgv, wd

mvxspjswz.

Hint: Something about missiles and error. There's a remix of this text on Youtube you can look up for giggles.
For your convenience:

Letter	Counts	Fraction	Letter	Counts	Fraction
a	0	0.00%	n	0	0.00%
b	0	0.00%	o	3	1.65%
c	10	5.49%	p	8	4.40%
d	15	8.24%	q	4	2.20%
e	4	2.20%	r	10	5.49%
f	0	0.00%	s	26	14.29%
g	4	2.20%	t	3	1.65%
h	4	2.20%	u	2	1.10%
i	1	0.55%	v	25	13.74%
j	21	11.54%	w	9	4.95%
k	2	1.10%	x	2	1.10%
l	17	9.34%	y	0	0.00%
m	2	1.10%	z	10	5.49%

2. Affine encryption [200 pts]:

Use the key {*a* = 3, *b* = 4} to encode the plaintext below. *a* is the scaling factor (or slope, if you prefer), and *b* is the bias term (or intercept/offset). Terms below are provided for your information but do not need to be encoded.

Plaintext:

```
    Elliptic curve cryptography is used for
SSH*, TLS**, and bitcoin.
```

*Secure Shell - interface for accessing other computers via network.

**Transport Layer Security - protocol used for most network communication like web browsing and email.

3. Affine encryption [200 pts]:

Use the key {*a* = 25, *b* = 17} to encode the plaintext.

Plaintext:

```
We are adders, so we need a log table to
multiply.
```

4. Vigenère encryption [300 pts]:

Use the keyword `mho` to encode the plaintext.

Plaintext:

```
Alessandro resisted the circuitous
inductance into a shockingly negative
secret society.
```

5. Vigenère decryption [300 pts]:

Use the keyword `ironic` to decode the following ciphertext.

Ciphertext:

```
Q kvbcipk bbb kbj bbb c akceg vpv xrlk
efiyl vmcz lww qkg n akby zrogvu.
```

6. Spanish Caesar decryption [300 pts]:

The following ciphertext was encoded using a Caesar shift of 14, so you should use a shift of +12 to decode it.

Note: for simplicity, accent marks have been omitted from plaintext (and also ciphertext)

Ciphertext:

Zo awhcqcbrfwo sg zo dchsbqwo rs zo qszizo

7. Baconian Cipher decryption [400 pts]:

Use the following table to decode the message hidden in the suspect sentence below. You can ignore the last five letters since they are not defined by the table.

Say B corresponds to lower case and A to upper case.

Example: cODeS becomes bAAbA which is 's' in our table.

AAAAA	a	AbbAb	n
AAAAb	b	AbbbA	o
AAAbA	c	Abbbb	p
AAAbb	d	bAAAA	q
AAbAA	e	bAAAb	r
AAbAb	f	bAAbA	s
AAbbA	g	bAAbb	t
AAbbb	h	bAbAA	u
AbAAA	i	bAbAb	v
AbAAb	j	bAbbA	w
AbAbA	k	bAbbb	x
AbAbb	l	bbAAA	y
AbbAA	m	bbAAb	z

Sentence with hidden message in it:

tHErE iSAbs OLuTE LYnoT HINGS UspIc IousT OSeeI nTHIs TOTAL Lyinn OCent LoOKI NGMES ssage.

8. Caesar cryptanalysis [500 pts]:

Ciphertext:

Hss nhbs pz kpcpklk puav aoyll whyaz, vul vm dopjo aol ilsnhl puohipa, aol hxbp ahup huvaoly, huk nhbsz (ruvdu hz jlsaz pu aolpy shunbhnl) aol aopyk.

9. Mystery cryptanalysis [500 pts]:

Ciphertext:

Bjo zjtao hsmc jrfpjeel j dssc okl yx ga bjo os xjtspo jmc xejogl?

State-level questions [1300 pts]

10. RSA decryption [400 pts]:

For this problem, use an alphabet starting with ‘a’ = 0, ‘b’ = 1, ..., ‘z’ = 25 and decrypt each letter separately using the key provided.
Note: this just defines a glorified monoalphabetic substitution. There are only 6 unique letters.

Use the key: $e = 5$, $N = 26$ where *Decrypt(y)* = $(y^e \text{ mod } N)$ yields the original character.
Ciphertext:

Lkhho plkxk

Hint: $x^5 (mod\ N) \equiv x^4 \cdot x$ (mod N), and $x^4 \equiv (x^2 \text{ mod } N)^2$ (mod N). This approach is known as repeated squaring since it only involves the raising x to a few powers of 2 and multiplying some of those results together (in this case x^1 and x^4, but if we chose $e = 7$, we’d use x^1, x^2, and x^4).

11. Hill Cipher decryption [300 pts]:

Use the decryption matrix on the right to multiply column matrices formed by three-letter chunks of the encoded message.

$$\text{Matrix: } \begin{pmatrix} 5 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

Ciphertext:

gcj uwq yvi

12. Vigenère with crib cryptanalysis [300 pts]:

Suppose we know that this message uses a key of length 6 and that we know the first 7 letters of the plaintext message. Find the original message.

First 7 letters: Weather
Ciphertext:

```
Srsnven vk minjl lirau omn preay uzaj
gmlwnc vf wosa.
```

13. Affine Cipher decryption [300 pts]:

The following ciphertext was encoded using the key {*a* = -5, *b* = ???}.
Hint 1: Not knowing *b* essentially makes this into a Caesar cryptanalysis question, but it's not so bad since we know that "`p`" is a one-letter word...
Hint 2: (-5) * (+5) = -25 = (-26)+1
Ciphertext:

```
Gpov p lcvbdd pca dxapmbyvqtm apz!
```