Raw Score: _____/4000

Rank: _____

Codebusters C

CPS Regionals @ IIT
Saturday, March 16, 2019

Instructions:

1. Don't open this test until told
2. You can start filling out your team/names below
3. If you tear the test, write your team name on every page.
4. This test uses the convention that 'a' = 0, 'b' = 1, ... 'z' = 25 for any Affine Cipher and Hill Cipher questions. The rest of the questions shouldn't require a distinction.
5. There are 12 questions. Questions 5,6, and 7 have extra (short) questions intended to cover more interesting material while still being related to understanding encryption/decryption.
6. Good Luck!

Team Name: _____

Team Number: _____

Names: _____

Timed Question (Aristocrats):

1. Aristocrats Cryptanalysis [500 pts + 2400 max time bonus]

Counts or letter mappings (you can fill out if you want -- provided just for convenience)

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 lbpp uo ta jo jqc rbifbwuczcv nsw swv rsy

qcppo ny wsnc br bwbuo nowjoys yot gbppcv ny

fsjqcz azcaszc jo vbc

Team Number: _____

2. Atbash. [200 pts]

```
Gsv mvcg xlwv dzh vmxlwvw drgs z xzvhzi hsrug lu gsrigvvm.
```

3. Mystery. [300 pts]

```
Crbcyr qbag guvax gur havirefr or yvxr vg vf ohg vg qb.
```

4. Aristocrats encryption. [300 pts] Encrypt using the following lookup table.
Plaintext letters on top map onto ciphertext letters on the bottom row.

In	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
Out	i	u	h	z	w	t	q	l	m	y	c	e	r	v	d	k	p	n	o	f	s	a	g	j	b	x

```
Shor's quantum factoring algorithm can crack both RSA and ECC.
```

5. Affine encryption
a. [300 pts] Encrypt the plaintext with the key *a= -1, b = 1*. *Convention: E(x) = ((a*x + b)* mod *26).*

```
Atbash and Caesar are special cases of Affine. Change my mind.
```

b. [50 pts] This (Affine cipher w/ *a = -1, b = 1*) is equivalent to applying Atbash and then Caesar shifting. What <u>shift</u> would be used for that Caesar shift? *Hint: What does the Atbash cipher look like when expressed as an affine cipher?*

6. Vigenère Decryption – decryption key "`doit`"

a. [300 pts] Apply "`do it`" to

`Qtaz zuhobd opix ehhq s mfzw hapaafaf al yq jlxdlzfavk.`

b. [50 pts]What was the encryption key that corresponds with "`do it`" ? That is, what codeword did I use to find the ciphertext given in part a?

7. Aristocrats cryptanalysis

a. [500 pts]Find the original sentence:

`Gqr rwbtksa rwoejzgbcw nsa nrsmre gqsw gqr trekswa gqcltqg.`

b. [100 pts] The previous part was encoded using an "involutary permutation" similar to what the Enigma machine would have used. It's slightly different because there is a single monoalphabetic substitution, while the Enigma would have used a different substitution for the 1st, 2nd, ... etc. letters of the plaintext.

An "involutary permutation" *f* is a mapping of plaintext letters to ciphertext letters such if *f(x) = y*, then *f(y) = x* for any letter represented by *x*. That is, *f* is its own inverse.

What would happen if we re-encoded the ciphertext given in 7a using the encryption key? Just give a quick qualitative answer. *Hint: what is f(f(x))?*

Note: The Engima used a different such mapping for each letter, which made it harder to crack. But the restrictions mentioned above made it easier to crack than originally thought.

Team Number: _____

8. Vigenère encryption [300 pts] with "etm" (for electron, tau, muon – the three types of neutrinos)

```
Neutrinos can switch types.
```

9. Hill Cipher encryption [200 pts]:

Encryption matrix: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

```
Go Linear Algebra!
```

Hint: Avoid doing arithmetic or letter-number conversions!

10. Hill Cipher Key inversion [300 pts].

What if we have a 2x2 encryption matrix and we want to find the decryption matrix? Note that we're working in base 29 this time! I've provided multiplicative inverses modulo 29 in a table below. (Having a prime base is nice because the multiplicative inverse is always defined)

Find the decryption matrix (which is the inverse of the encryption matrix) and state it with each entry between -28 and +28. I'm fine with negatives since they can be easier to deal with.

$$\text{Find } \begin{pmatrix} 3 & -5 \\ 6 & 17 \end{pmatrix}^{-1} \pmod{29} \qquad \text{Hint: } \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \equiv \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{29}$$

Lookup table for multiplicative inverses modulo 29 (only use for the determinant):

n	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
n^(-1)	1	15	10	22	6	5	25	11	13	3	8	17	9	27	2	20	12	21	26	16	18	4	24	23	7	19	14	28

11. Vigenère decryption [300 pts] using code "box"

Rokqahcuqfqur ods vxrf zzzwr mwsqqsurm.

12. Affine Decryption [300 pts]
Using *a=3, b= -3* -- Use *D(y) = ((a*y + b)* mod *26)* as though you were encrypting, even though the input is clearly the ciphertext.

Qvflh uzo rmlo jxzyl mbivod uwvlh.