# SOLUTIONS



1. (5 pts) Decrypt the following message, which was enciphered using the Atbash cipher.

DVOO YVTFM RH SZOU WLMV

(not covered yet)

2. (7 pts) A ciphertext was enciphered using an affine cipher. Given that the ciphertext letters I and J correspond to the plaintext letters T and I, respectively, find the encipherment formula.

$19$ T $\hookrightarrow$ I $8$

$8$ I $\hookrightarrow$ J $9$

Affine cipher equation

$$y \equiv ax + b \pmod{26}$$

Solve the system for a & b

$$8 \equiv 19a + b \pmod{26}$$

$$-(9 \equiv 8a + b \pmod{26})$$

$$-1 \equiv 11a \pmod{26} \qquad 11^{-1} \equiv 19 \equiv -7 \pmod{26}$$

Multiply both sides by $11^{-1} \equiv -7 \pmod{26}$

$$7 \equiv a \pmod{26}.$$

Then, $9 \equiv 8 \cdot 7 + b \pmod{26}$ so $b \equiv 9 - 56 \pmod{26}$

$\equiv 5 \pmod{26}$.

Finally, the formula is

$$y \equiv 7x + 5 \pmod{26}$$

Check T & I satisfy: $8 \equiv 7 \cdot 19 + 5 \equiv 7(-7) + 5 \equiv -44 \equiv 8 \pmod{26}$ ✓

3. (8 pts) A simple columnar transposition was used to produce the ciphertext

OGASE NSENV GURTT AELSG IUREE WKSII INP

Decipher the message. Show your work.

33 letters - Probably 3 or 11 columns.

If there were 11 columns, we'd have 3 rows,

O S S V
G E E G
A N N U

which is not English.

We try 3 colums of 11 letters:

O U R
G R E
A T E
S T W
E A K
N E S
S L I
E S I
N G I
V I N
G U P

Message: Our greatest weakness lies in giving up.

4. Consider the following Vigenère-encipherered text:

```
ICFXF PCCXM FZTHL TKGHH LXHST GXBFL
LVIMY CGHML EMQZI KZLIV IFZLS HSLLD
USVMY CHZMG XQPBH TIPDK WHWMJ HVTXC
DIWYF PIIRX FPICX TBCPF QLREP WRLKY
HSEHW RGCYU CCHOR WSWDD THJGC UIGUR
WSQ
```

(a) (4 pts) Use the Kasiski test to determine the most likely length(s) for the keyword. (**Hint**: The trigraphs XFP, MYC and FPI appear twice in the above ciphertext. Their occurrences are underlined.)

XFP: 96 letters apart
MYC: 30 letters apart
FPI: 6 letters apart.

Most likely length(s) divide gcd(6,30,96)=6
So 2, 3, or 6 are most likely.

(b) (6 pts) Determine the keyword given that the end of the plaintext reads: "...END THEM."

$I^{8}\ G^{6}\ U^{20}\ R^{17}\ W^{22}\ S^{18}\ Q^{16}$

$E^{4}\ N^{13}\ D^{3}\ T^{19}\ H^{7}\ E^{4}\ M^{12}$

We suspect that the keyword is 6 letters long, as the first & seventh letters of this group are encrypted by the same shift.

G → N by subtracting 19 (mod 26): T
U → D 17 R
R → T -2≡24 Y
W → H 15 P
S → E 14 O
Q → M 4 E

Keyword
TRY POE

5. (10 points) Decrypt the following English sentence, which was encrypted using a shift cipher.

   THEMO STCER.TAINWAYTOS UCCEE DIGAL WAYST OTRYJ USTON EMORETIME
   BPMUW ABKMZ BIQVE IGBWA CKKMM LQAIT EIGAB WBZGR CABWV MUWZM BQUM

   Show your work.
   **Hint**: The most frequent ciphertext letters are B and M, which appear eight (8) and seven (7) times, respectively.

B + M are $11 \equiv -15 \pmod{26}$ apart.

Our most frequent letters are E, T, N, O, R, I, A.

We see T + I are 11 apart, but E + T are 15 apart. Trying B → I, M → T, we get the first letters IWTB which is not English.

However B → T, M → E, which is a shift of +18 for decipherment gives

P: $15 + 18 \equiv 7 \pmod{26}$ → H
U: $20 + 18 \equiv 12 \pmod{26}$ → M
W: $22 + 18 \equiv 14 \pmod{26}$ → O

Message:

The most certain way to succeed is always to try just one more time.

6. (10 pts) The following text was encrypted using a keyword to obtain a mixed alphabet.

JGFUU VUPYR BCKAG QQCJM HUGQM LQQCE HUETR KLRQC JMHUP
MAKEEVERYT HINGA SS M EASP SS E T N TSIMPLER

The beginning segment of the plaintext reads: "MAKE EVERYTHING ...". Decrypt the message and recover the keyword. Explain your method.

From the first two words, we recover:

| Plain | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher | G | E | | | U | | A | B | | F | J | K | | | | P | | R | | V | | | | | Y | |
| 2nd rd: | | | C | D | | | | H | | | | L | M | | | | Q | | T | | | W | X | | | Z |

We can see this must be a simple substitution. After V, the alphabet must stay the same.

Also, S must become Q + U must be S or T and the other letter must be in the keyword. Filling in letters we know we get

Make everything as S_M--E, so we guess

| Cipher | Plain |
|---|---|
| C | I |
| M | P |
| H | L |
| L | O |

Make everything as simple as possi_le
↑ must be b

Cipher Plain
B → E

We guess "but not" are the next words.

Phrase: Make everything as simple as possible but not simpler.

Letters in keyword are missing in the rest of the alphabet, so

The numerical Equivalents of the letters of the English alphabet are

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Inverses modulo 26

| $a$ | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{-1}$ MOD 26 | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

We have

| Plain | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cipher | G | E | | | U | | | A | B | C | D | | F | H | J | K | L | M | | P | Q | R | T | | V | W | X | Y | Z |

Keyword letters left: I, S, & N or O

To make a word g e – – u – , we use n, i, & s to have Keyword GENIUS