SOLUTIONS

Question 1. (6 points each) Solve for x:

(a) $x + 4 \equiv 2 \pmod 7$

$-4 \quad -4$

$x \equiv -2 \equiv 5 \pmod 7$

(b) $3x - 4 \equiv 4 \pmod{11}$

$3x \equiv 8 \pmod{11}$ ... $3^{-1} \equiv 4 \pmod{11}$ as $3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$

So $x \equiv 4 \cdot 8 \equiv 32 \equiv 10 \pmod{11}$

$x \equiv 10 \pmod{11}$

Question 2. (15 points) Decipher the following text which was enciphered using a shift cipher. Word spacings have NOT been preserved.

MAXPHK WLMHKR BLWXYB GXWTLM AXGTKK TMBGZH KKXETM BGZHYT GXOXGM HKLXKB XLHYXO
XGMLMA TMTKXX BMAXKM KNXHKY BVMBMB HNL

Frequency
M 13
X 12
H 5
K 10

E + T are most common + 15 letters apart. From M to X is only 11, but from X to M is 15. We guess T → M, and it works (see below).

Message: The word story is defined as: the narrating or relating of an event or series of events that are either true or fictious.

For your use, if you would like:

	0	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
Cipher	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
Plain	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

CONTINUE TO NEXT PAGE

Question 3. (10 points) Encrypt the following sentence using **a keyword columnar transposition** cipher, with the keyword MAYBE.

THINK TWO GOOD THOUGHTS

④	①	⑤	②	③
M	A	Y	B	E
T	H	I	N	K
T	W	O	G	O
O	O	T	H	O
U	G	H	T	S

Message: HWDG NGHT KOOS TTOU IOTH

Question 4. (6 points) Solve the following system of congruences:

$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 8$$

We must find x_1 with

$8x_1 \equiv 1 \pmod 5 \longrightarrow 3x_1 \equiv 1 \pmod 5$

so $x_1 \equiv 2 \pmod 5$.

$5x_2 \equiv 1 \pmod 8$ and $5 \cdot 5 = 25 \equiv 1 \pmod 8$

so $x_2 \equiv 5 \pmod 8$.

Then $x \equiv 3 \cdot 8 \cdot 2 + 1 \cdot 5 \cdot 5 \pmod{40}$

$\equiv 48 + 25 \pmod{40}$

$x \equiv 33 \pmod{40}$

CONTINUE TO NEXT PAGE

Question 5. (4 points each)

(a) Give an example of one stronger keyword and one weaker keyword for the Vigenere Cipher and explain your choices.

A stronger keyword would be XZDFJPEN, because it has 8 different letters and is not an English word (so not easily guessed).

A weaker keyword would be ADAM, since it repeats the letter A and the 1st and 3rd letters would not be encrypted at all.

(b) Give 3 integer values of n, including at least one positive and one negative integer, that satisfy the following congruence:

$$n + 3 \equiv 2 \pmod{15}$$

$n \equiv -1 \pmod{15}$

Possible values

$n = -1, -16, -31, -46, 14, 29, 44, 69, \ldots$

(c) When trying to decrypt the following substitution cipher, state 2 methods that you would use. YOU DO NOT NEED TO ENTIRELY DECRYPT THE MESSAGE.

ZLE ZXEE N$ M VHMSZ

(1) The letter M is a word, so it must be the letter I or A.

(2) The letters Z & E are most frequent, with ZLE at the beginning of the sentence. These may be T & E respectively.

(3) The two letter word NY could be a verb IS.

CONTINUE TO NEXT PAGE

Question 6. In the English alphabet, we know the seven most common letters are

`E, T, N, O, R, I, A.`

(a) (4 points) How many different 2 letter "words" could we make using these letters, where a double letter is not considered a "word"?

We must pick two letters. For the first, we have 7 choices. For the second, only 6 choices left as we cannot repeat. We have $P(7, 2) = 7 \cdot 6 = \boxed{42 \text{ words}}$

(b) (6 points) Suppose these 7 letters made up an entire alphabet, where each letter is as likely as any other. What is the probability that the letter `T` is one of the two most frequent letters in a text?

There are 6 ways to choose the other most frequent letter, and $\binom{7}{2} = \frac{7 \cdot 6}{2} = 21$ ways to pick 2 letters.

$$\text{Prob} = \frac{6}{21} = \boxed{\frac{2}{7}}$$

CONTINUE TO NEXT PAGE

To; Continued

JO DH DHUH LHFSI IZ GZG
IF WE WERE MEANT TO POP

ZPI ZO MHA DH'A BEHHG
OUT OF BED WE'D SLEEP

JS IZFBIHUB.
IN TOASTERS.

Decryption formula:

$X \equiv 15(Y-5) \pmod{26} \equiv 15Y + 3 \pmod{26}$

J: 9 $X \equiv 15 \cdot 9 + 3 \pmod{26} \equiv 138 \equiv 8 \pmod{26}$

J → I

D: 3 $X \equiv 15 \cdot 3 + 3 \equiv 48 \equiv 22 \pmod{26} \rightarrow W$

U → R
O → F
P → U

by English words

G: 6 $X \equiv 15 \cdot 6 + 3 \equiv 93 \equiv 15 \pmod{26} \rightarrow P$

B: 1 $X \equiv 15 + 3 \equiv 18 \pmod{26} \rightarrow S$

F → A
E → L
S → N
L → M
A → D

Message:

If we were meant to pop out of bed, we'd sleep in toasters.

Question 7 The following text is encrypted with an affine cipher, with word divisions preserved.

E E E E T T T
JO DH DHUH LHFSI IZ GZG ZPI ZO MHA DH'A BEHHG JS IZFBIHUB

You may use that the most frequent ciphertext letters are H and I.

(a) (15 points) Give the **encryption OR decryption** formula, and decipher the message. Be sure to label (encryption or decryption) which formula you give!

Letter #
H → 7
I → 8

H is more frequent than I, so we try
$^{7}H \to {}^{4}E$
$^{8}I \to {}^{19}T$

Also, we have two letter words that end in E (to go with DH), but no two letter words that begin with E (if IZ $\leftrightarrow$ E_).

Solving
$-(7 \equiv 4a + b \pmod{26})$
$8 \equiv 19a + b \pmod{26}$
$1 \equiv 15a \pmod{26}$
so $a \equiv 15^{-1} \equiv 7 \pmod{26}$

Then $7 \equiv 4 \cdot 7 + b \pmod{26}$
$b \equiv -21 \equiv 5 \pmod{26}$

Encryption Formula:
$Y \equiv 7x + 5 \pmod{26}$

(b) (4 points) Could the most frequent ciphertext letters correspond to plaintext letters N and R? Why or why not?

No, they could not. If H → N, I → R, we'd have the system

$7 \equiv 13a + b \pmod{26}$
$8 \equiv 17a + b \pmod{26}$
$1 \equiv 4a \pmod{26}$.

a would need to be the inverse of 4 mod 26, which does not exist. Thus, this could not be an affine cipher.

CONTINUE TO NEXT PAGE

Question 8 The following message is encrypted using the Vigenere cipher.

XHUE HMMO PPLR OVAA IPKS BRGQ UHJL GHKR IPNB RFQY FETK VGHA
VHYE CVZL OINS LSRC IBPI VPXW TJHM MSVY TMNK UZSR KULX RWJM
MOPI NXIU YTXH GYTQ AMPG KVKZ BFLG DAET KZAM DFLG ESCZ

(a) (6 points) There are 3 repeated strings in the text above. The string `HMM` appears twice, 70 characters apart. The string `MMOP` appears twice, 90 characters apart.

The string `FLG` appears twice. How many character apart are the two occurrences? Given these repetitions, what possible length(s) could the keyword have and why?

FLG: Appears 10 characters apart

The keyword length will probably divide the gcd(10, 70, 90) = 10 by the Kasiski Test. Thus, the keyword most likely has length

2, 5, or 10.

(b) (10 points) If you know that the first words are "Education is", find the keyword used to encrypt the message.

23 → X T H U E H M M O P P L
A A
4 E D U C A T I O N I S

X → E: 23 − 4 ≡ 19 (mod 26) → T
H → D: 7 − 3 ≡ 4 (mod 26) → E
U → U: 20 − 20 ≡ 0 (mod 26) → A
E → C: 4 − 2 ≡ 2 (mod 26) → C
H → A: 7 − 0 ≡ 7 (mod 26) → H

Checking we see the next 5 letters have the same shift.

Keyword: TEACH

THIS IS THE LAST QUESTION. RESOURCES ARE ON THE NEXT PAGE.