Coding Theory and Cryptography: HW 4

Paridhi Latawa

March 21, 2021

Abstract

This materials covers classical and symmetric key cryptosystems. Readings and practice problems covered are the following.

1. Module: Public Key Cryptography and the RSA Cryptosystem, pages 3-7. Problems: 2, 3, 4, 5.

2. Chapter 2 of Trappe and Washington. Problems: 2, 3, 4, 5, 6, 7, 13, 14, 17

3. Hankerson Section 10.1 and 10.2. Problem: 10.2.5.

1 Public Key Cryptography and the RSA Cryptosystem, page 3 - 7

Problem 2: Is there a value of k for the shift cipher on the English alphabet for which the encryption and decryption functions are identical?

It could be the same for k = 26.

Problem 3: What is the size of the key space for the substitution cipher on the English alphabet?

The keyspace should be (26)! as each letter that is being converted from the plaintext can be assigned any of the 26 letters. With b, there are 25 possible values it can take on (as it is excluding what a is assigned to). Going through the alphabet, we end up with 26! as the size of a keyspace.

Problem 4: Given that the following text is encrypted using a substitution cipher, decrypt the ciphertext and determine the encryption key (permutation). There are no spaces or punctuation marks in the text.

Ciphertext:

FOEWZKNTZGKSBLNTZJOZZFGMEVNTZEVNHXLTVKYSNTGOATNNTVNHNQGO
DYTVPZVWLGDONZDSFGIKVXNHXVDVIIDHXVNHGFLNTZKLVXKSINGLSLNZEV
FYGNTZKVIIDHXVNHGFLGMFOEWZKNTZGKSIKGPZYNTHLAKZVNEVNTZEVNH
XHVFQKGFA

We see that the trigram NTZ has the highest frequency in this ciphertext. We can allocate that with the.

After attempting various substitution cryptosystems, we can conclude that this is a monoalphabetic substitution.

By looking at frequencies, we can further deduce the message, which comes out to be:

NUMBERTHEORYISTHEQUEENOFMATHEMATICSHARDYTHOUG HTTHATIT-
WOULDHAVEABSOLUTELYNOPRACTICALAPPLIC ATIONSTHERSACRSV-
TOSYSTEMANYOTHERAPPLICATIONSOF NUMBERTHEORYPROVEDTHIS-
GREATMATHEMATICIANWRONG

This is the acquired substition:

A	G
B	I
C	
D	L
E	M
F	N
G	O
H	I
I	P
J	Q
K	R
L	S
M	F
N	T
O	U
P	V
Q	W
R	
S	Y
T	H
U	
V	A
W	B
X	C
Y	D
Z	E

Problem 5: Explain what happens if two messages are encrypted with the same key in Vernam cipher.

In Vernam ciphers, the keys should be chosen randomly and then only used once. If a key was used to encrypt two messages, the Vernam cipher could be not as unconditionally secure against attacks. As mentioned in the module, when keys were used multiple times, it allowed for messages to be cracked (ex. using the VENONA project).

2 Trappe and Washington: Chapter 2 - Classical Crytosystems

Problem 2: The ciphertext UCR was encrypted using the affine function $9x + 2$ mod 26. Find the plaintext.

We start with $y = 9x + 2$ and further solve $x = \frac{1}{9}(y - 2)$. $\frac{1}{9}$ is reinterpreted when we work with mod 26. Since $\gcd(9, 26) = 1$, there's a multiplicative inverse for 9 mod 26. $9 * 3 \equiv 1 \pmod{26}$, so 3 is the desired inverse and can be used in place of 1/9. So,

$x \equiv 3(y - 2) \equiv 3y - 6 \equiv 3y + 20 \pmod{26}$

We then convert the above message using the above equation.

U(=20) is mapped to $3 * 20 + 20 = 80 = 2 \pmod{26}$, which is the letter C.

C(=2) is mapped to $3 * 2 + 20 = 26 = 0 \pmod{26}$, which is the letter A.

R(=17) is mapped to $3 * 17 + 20 = 71 = 19 \pmod{26}$, which is the letter T.

The decoded message is cat.

Problem 3: Encrypt *howareyou* using the affine function $5x + 7 \pmod{26}$. What is the decryption function? Check that it works.

To encrypt using the Affine Cipher, we take the plaintext letters and input their numerical equivalent into the provided function. This will give us the corresponding numerical value for the decoded phrase.

h(=7), which is encrypted to $5 * 7 + 7 = 42 = 16 \pmod{26}$, which is the letter Q

o(=14), which is encrypted to $5 * 14 + 7 = 77 = 25 \pmod{26}$, which is the letter Z

w(=22), which is encrypted to $5 * 22 + 7 = 117 = 13 \pmod{26}$, which is the letter N

a(=0), which is encrypted to $5 * 0 + 7 = 7 \pmod{26}$, which is the letter H

r(=17), which is encrypted to $5 * 17 + 7 = 92 = 14 \pmod{26}$, which is the letter O

e(=4), which is encrypted to $5 * 4 + 7 = 27 = 1 \pmod{26}$, which is the letter B

y(=24), which is encrypted to $5 * 24 + 7 = 127 = 23 \pmod{26}$, which is the letter X

o(=14), which is encrypted to $5 * 14 + 7 = 77 = 25 \pmod{26}$, which is the letter Z

u(=20), which is encrypted to $5 * 20 + 7 = 107 = 3 \pmod{26}$, which is the letter D

So, the entire ciphertext is QZNHOBXZD

Problem 4: Consider an affine cipher (mod 26). You do a chosen plaintext attack using *hahaha*. The ciphertext is $NONONO$. Determine the encryption function.

Given the above, we can deduce that 7 (=h) maps to 13 (=N), and 0 (=a) maps to 14 (=O).

Therefore, we have the equations

$7\alpha + \beta \equiv 13 \pmod{26}$

$\beta \equiv 14 \pmod{26}$

Subtracting yields

$7\alpha \equiv -1 \equiv 25 \pmod{26}$

This has the unique solution $\alpha = 11$

Using the first equation, $7 * 11 + \beta \equiv 13 \pmod{26}$ which yields $\beta = 6$

Problem 5: The following ciphertext was encrypted by an affine cipher mod 26: $CRWWZ$. The plaintext starts ha. Decrypt the message.

So C (=2) corresponds with h (=7) and R (=17) corresponds with a (=0).

We get the equations,

$7\alpha + \beta \equiv 2 \pmod{26}$

$\beta \equiv 17 \pmod{26}$

Subtracting these equations, we get

$7\alpha \equiv -15 \pmod{26}$

This has the unique solution $\alpha = 9$.

Inputting this into the second equation,

we simply get that $\beta = 17$

The affine function equation is then

$9x + 17 \pmod{26}$

As we are decrypting, we need to find the inverse of the above equation. The inverse is

$\frac{1}{9}(x - 17) \pmod{26}$

We know that 3 is the multiplicative inverse for 9 (mod 26), so we get

$3(x - 17) \pmod{26}$

Decoding the rest of the message, we get:

W (=22) maps to 3(22 - 17) (mod 26) = 15 (mod 26), which is the letter P. There are two Ws.

Z (=25) maps to 3(25 - 17) (mod 26) = 24 (mod 26), which is the letter Y.

So, the entire plaintext is "happy"

Problem 6: Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

The result would be a larger culminating affine function, which could take more time to decrypt or use.

Problem 7: Suppose we work with mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if we work mod 29?

If we were to use mod 27, we would have to choose two integers α and β that fit $\gcd(\alpha, 27) = 1$. More multiples would be excluded so there would be fewer possible values for α. All multiples of 3 would not be possible as then the gcd would be greater than 1. So that means the possible values of α are 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, and 26. That is 18 different possible values for α. There are 27 different possible values for β. In total, there would be 27*18 values for the key.

If we were to use mod 29, we would similarly have to choose two integers α and β that fit $\gcd(\alpha, 29) = 1$. 29 has no multiples besides 1 and itself as it is a prime number, so the total number of possible keys is 28*29, as we exclude 29 in the possibilities for values for α.

Problem 13: The ciphertext YIFZMA was encrypted by a Hill cipher with the matrix below. Find the plaintext.

$$\begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}$$

Problem 14: The ciphertext text GEZXDS was encrypted by a Hill cipher with a 2 x 2 matrix. The plaintext is *solved*. Find the encryption matrix M.

Problem 17: Suppose the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is used for an encryption matrix in a Hill cipher. Find two plaintexts that encrypt to the same ciphertext.

Take ab as one of the plaintexts. Encrypting that, we get

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \end{bmatrix}$$

The ciphertext is DE.

We can add 26 to $\begin{bmatrix}3 & 4\end{bmatrix}$ to find another possible plaintext that encrypts to the same ciphertext as above.

So, we get the following scenario in which we need to solve for x and y.

$$\begin{bmatrix}x & y\end{bmatrix} \begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}29 & 30\end{bmatrix}$$

We can write this as a systems of equations:

$x + 2y = 29$

2x + 4y = 30

Solving the system of equations, we get x = -13 and y = 14.

When inputting these values for x and y, we get the resulting ciphertext numerical values as $\begin{bmatrix}55 & 82\end{bmatrix}$

Taking this matrix with mod 26, we get numerical values that equate to DE as the ciphertext.

3 Hankerson: Section 10.1 and 10.2

Problem 10.2.5: The following ciphertext was obtained under a Vigenere cipher of the type discussed in Example 10.2.3. Recover the key word of the cipher, given that the underlined triple of letters represents a very common three-letter word, and that the overscored letters 'AE' represents the combination 'an' at the beginning of a three-letter word.

Offset and Ciphertxt:

0 VHVVG NRWGA EGCLJ RVHVO GAUHT OWWJE FSROJ LVIFQ KNKKG IIDPG

50 VUJAM HLUJW CLCRY EUWJE DVGLM HUBFW JTFEG CFPGV LOPEI DDLVW

100 QOLUE ALVGM VVJAC OCTKD EKKKG MRVBE BHRLR QPEUW QMFUT ONLPD

150 RBNIX KVBLM

Using the Kasiski test and the information provided in the question, the distance between the two VHVs is $16 = 2^2 * 4$

The distance between the two WJEs is $40 = 2^2 * 10$.

So the length is most likely 4.

After looking at frequency analysis based on the key that we have now deduced.

We can assume that VHV is 'the' as this is one of the most common trigraphs in the English language.

If V and G are shifted the same amount, we can determine that V is shifted by 2.

So by shifting every first, fifth, ninth, etc. term in the sequence, we are able to find some more letters. Again, inputting VHV as 'the' and deducing that the 'an' provided in the question actually forms the larger word 'and', we can further deduce the shifts in the key.

From that, the plaintext is deduced as the following.

the senate and also the leaders of the opposition in their anger have just allowed themselves both to become vulnerable to our cause me shall attack them as zeke planned tomorrow in daylight buj

The key is card.

]