CIS 628 Homework 1 - Part 1

Introduction to Cryptography

Syracuse University

Fall 2022

Homework 1

Name: Saket Kiran Thombre

SU ID: 899913802

NetID: sthombre

Email: sthombre@syr.edu

1.1 (10 points) The following ciphertext was the output of a shift cipher: ycvejqwhqtdtvmm What is the key and what is the decrypted plaintext?

Solution:

Given ciphertext = “ycvejqwhqtdtvmm”

The plaintext is encrypted using a shift cipher. A shift cipher is a substitution cipher where we shift the letters by one or more values in the English alphabet series. We use a alphabet and a key to shift the letter positions.

Since we don’t know the key, we are going to brute force the ciphertext against all possible shifts in the English alphabet set.

Shifts	Sr No.	Possible plaintext
1	(25)	xbudipvgpscsull
2	(24)	watchouforbrtkk
3	(23)	vzsbgntenqaqsjj
4	(22)	uyrafmsdmpzprii
5	(21)	txqzelrcloyoqhh
6	(20)	swpydkqbknxnpgg
7	(19)	rvoxcjpajmwmoff
8	(18)	qunwbiozilvlnee
9	(17)	ptmvahnyhkukmdd
10	(16)	osluzgmxgjtjlcc
11	(15)	nrktyflwfisikbb
12	(14)	mqjsxekvehrhjaa
13	(13)	lpirwdjudgqgizz
14	(12)	kohqvcitcfpfhyy
15	(11)	jngpubhsbeoegxx
16	(10)	imfotagradndfww
17	(9)	hlenszfqzcmcevv
18	(8)	gkdmryepyblbduu
19	(7)	fjclqxdoxakactt
20	(6)	eibkpwcnwzjzbss

21 (5) dhajovbmvyiyarr

22 (4) cgzinualuxhxzqq

23 (3) bfyhmtzktwgwypp

24 (2) aexglsyjsvfvxoo

25 (1) zdwfkrxirueuwnn

Seeing all the results, only shift by 2 makes a little sense i.e., “watchouforbrtkk”.

Since this is the only probable solution, we can say that the key length for the shift cipher is “2”.

Therefore, the plaintext is “watchouforbrtkk”.

1.2 (15 points) Suppose you have a language with only the 3 letters a, b, c, and they occur with frequencies .7, .2, .1, respectively. The following ciphertext was encrypted by the Vigenere method (shifts are mod 3 instead of mod 26, of course): ABCBABBBAC. Suppose you are told that the key length is 1, 2, or 3. (a) Show that the key length is probably 2 and determine the most probable key. and (b) decrypt the message.

Solution:

Given Ciphertext: ABCBABBBAC

Original Ciphertext	ABCBABBBAC	Counting Overlaps
Shift 01	ABCBABBBAC	2
Shift 02	ABCBABBBAC	3
Shift 03	ABCBABBBAC	1

As given in the problem shifts are mod 3, hence we compare ABCBABBBAC with shift 1,2 and 3. After shifting it, we check for overlaps.

After checking for overlaps, we observe that shift 2 has the highest number of overlaps. Since we now know that shift of 2 has the highest overlaps, hence we can safely say that we can look at alternate letters.

If its even, we get BBBBC where B has the highest frequency out of the total items in the set of 5. Hence, we can say that B would be encrypted from A.

If we check for odd, we get ACABA, where we get highest frequency for A, hence we can note that A will be encrypted from B.

Looking at the above observations, we can say that the key will be (B,A)

Hence, we can state the final answer as BAAABACABB by looking at the first few terms of the original ciphertext which are ABCBA

Now we can reverse calculate the answer EXOR with the key.

We get

Answer: BAAABACABB

EXOR BABABABABA

We get ABCBABBBAC

1.3 (10 points) Consider the shift cipher with the following distribution over M: Pr[M = kim] = 0.4, Pr[M = ann] = 0.3, Pr[M = boo] = 0.3. What is the probability that C = DQQ?

Solution:

We are given 3 probabilities

Pr [M = kim] = 0.4

Pr [M = ann] = 0.3

Pr [M = boo] = 0.3

We assume that all the sets Pr[M = kim], Pr [M = ann], Pr [M = boo] have equal probabilities of encryption.

So, we will calculate the probability of C = DQQ with Bayes theorem:

Pr[DQQ = ann] = (Pr[M = ann] * Pr[ann]) / (Pr [M=kim]*Pr[kim]) + (Pr[M = ann] * Pr[ann]) + (Pr[M = boo] * Pr[boo])

Pr[DQQ = ann] = (0.3 * 1/3) / ((0.4 * 1/3) + (0.3 * 1/3) + (0.3 * 1/3))

Pr[DQQ = ann] = 0.3

Similarly, we calculate for DQQ = boo

Pr[DQQ = boo] = (Pr[M = boo] * Pr[boo]) / (Pr [M=kim]*Pr[kim]) + (Pr[M = ann] * Pr[ann]) + (Pr[M = boo] * Pr[boo])

Pr[DQQ = boo] = (0.3 * 1/3) / ((0.4 * 1/3) + (0.3 * 1/3) + (0.3 * 1/3))

Pr[DQQ = ann] = 0.3

Now we know that Pr[M] = 1/26 since we are only considering English alphabets.

We can can further solve it to

(C = DQQ) = [0.3 * 1/26] + [0.3 * 1/26]

(C = DQQ) = 0.3/26 + 0.3/26

(C = DQQ) = 0.6/26

(C = DQQ) = 0.0230769231

Therefore, we can say that the probability of C = DQQ is 0.0230769231

1.4 (15 points) When using the one-time pad with the key k = 0 l , we have Enck(m) = k $\oplus$ m = m and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with k ≠ 0 l (i.e., to have Gen choose k uniformly from the set of nonzero keys of length l). Is this modified scheme still perfectly secret? Explain

Solution:

As we know that the one-time pad has a perfect secrecy property, that is we have no information about the original message from the given ciphertext.

Now let's suppose K = M = C = $\{0,1\}^n$

Where K is the key,

M = Original message

C = Ciphertext

If we try the suggested improvement and remove 0^n from the key pair space, we create a equation

|K| = |M| - 1 < |M|,

This contradicts the perfect secrecy principle because theoretically it is possible to encrypt a plaintext with a key 0^1.

Therefore, we cannot make any suggested improvements to the key pair space since it will reduce the perfect secrecy property.