Lea Middleton

ID# 1855452

CSC 440 Cryptology

1.14.2019

1.a)

CIPHERTEXT = “SKPEELAG”

Plaintext correspondence to ‘S’(numerical rep. of 18) = b( numerical rep. of 1)

Plaintext correspondence to ‘K’(numerical rep. of 10) = l( numerical rep. of 11)

Step 1) Subtract the system of congruent

Using formula , set up the system of congruent

|  |  |
| --- | --- |
|  | 1st equ |
| ─ |  |
|  | 2nd equ |
|  | 1st -2nd equ OR 3rd equ |

Step 2) Find the gcd(y1 – y2,n) gcd(8,26)

|  |  |  |  |
| --- | --- | --- | --- |
| Dividend | = | Divisor | Remainder |
| 26 | = | 8(3) | 2 |
| 8 | = | 4(2) | 0 |

gcd(8,26) = 2

Since the gcd(y,n) >1, divide the coefficients of the 3rd equation by 2

Step 3) Divide by 2 throughout 3rd equ and repeat Step 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| gcd(4,13) |  | Dividend | = | Divisor | Remainder |
|  |  | 13 | = | 4(3) | 1 |
|  |  | 4 | = | 2(2) | 0 |

nklkiublbhkj

Since gcd(4,13) = 1, solve

Step 4) Solve and solve for β from any of the equations from original system of congruent

Plug in α into one of the equations to solve for β, double check the results in the other equation

|  |  |  |
| --- | --- | --- |
|  | = | 11 |
|  | = | 11 |

**So…the encryption key (a,b) = (7,11)**

1.b) 1st. Find the multiplicative inverse of 7 mod 26. This number is 15

2nd. Formula to decrypt:

1.c)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CipherText |  |  |  | PlainText Correspondence |
| S | D(S) = 15(18 -11) mod 26 | = | 105 mod 26 = 1 | ‘b’ |
| K | D(S) = 15(10 -11) mod 26 | = | 15 mod 26 = 11 | ‘l’ |
| P | D(S) = 15(15 -11) mod 26 | = | 60 mod 26 = 8 | ‘i’ |
| E | D(S) = 15(04 -11) mod 26 | = | -105 mod 26 = 25 | ‘z’ |
| E | D(S) = 15(04 -11) mod 26 | = | -105 mod 26 = 25 | ‘z’ |
| L | D(S) = 15(11 -11) mod 26 | = | 0 mod 26 = 0 | ‘a’ |
| A | D(S) = 15(00 -11) mod 26 | = | -165 mod 26 = 17 | ‘r’ |
| G | D(S) = 15(06 -11) mod 26 | = | -75 mod 26 = 3 | ‘d’ |

**“SKPEELAG” = “blizzard”**

2)  **Exercise 6, page 55**

is the 1st affine function and is the 2nd affine function. To apply both to a plaintext, corresponds to… . This essential scaled

. This is just a single affine function of ax + b.

3.a) Encrypt ‘winter’ using the Hill Cipher

‘wi’ has numerical values w = 22, i = 8

‘nt’ has numerical values n = 13, t = 19

‘er’ has numerical values e = 4, r = 17

Using matrix multiplication, we obtain:

= =

= =

= =

Now take mod 26 to the resulting matrix:

14 = ‘O’, 16 = ‘Q’

3 = ‘D’, 14 = ‘O’

5 = ‘F’, 25 = ‘Z’

**“winter” = “OQDOFZ”**

3.b)

Step 1. Find determinate and then find if the gcd(det,n) = 1

Using an online calculator, the gcd(9,26) = 1

Step 2. Since the gcd(9,26) = 1, a.k.a the inverse of , can be obtained using the following formula:

Step 3. Take mod 26 to the resulting matrix from Step 2:

**The decrypt matrix:**

4.a) Using the program I wrote in assignment 1, the key length is 12

4.b) darwindarwin

4.c) Note: I broke up a couple of beginning lines and then the last few lines

Introduction when on board hms beagle as naturalist I was much struck with certain

Facts in the distribution of the inhabitants of south America and in the geological relations

Of the present to the past inhabitants of that continent these facts seemed to

Me to throw some light on the origin of species that mystery of mysteries as it has been

Called by one of our greatest philosophers on my return home it occurred to me in that

Something might perhaps be made out on this question by patiently accumulating and reflecting

onallsortsoffactswhichcouldpossiblyhaveanybearingonitafterfiveyears

workiallowedmyselftospeculateonthesubjectanddrewupsomeshortnotestheseien

largedinintoasketchoftheconclusionswhichthenseemedtomeprobablefromthatpe

riodtothepresentdayihavesteadilypursuedthesameobjectihopethatimaybeexcus

edforenteringonthesepersonaldetailsasigivethemtoshowthatihavenotbeenhast

yincomingtoadecisionmyworkisnownearlyfinishedbutasitwilltakemetwoorthree

moreyearstocompleteitandasmyhealthisfarfromstrongihavebeenurgedtopublish

thisabstractihavemoreespeciallybeeninducedtodothisasmrwallacewhoisnowstu

dyingthenaturalhistoryofthemalayarchipelagohasarrivedatalmostexactlythes

amegeneralconclusionsthatihaveontheoriginofspecieslastyearhesenttomeamem

oironthissubjectwitharequestthatiwouldforwardittosircharleslyellwhosenti

ttothelinneansocietyanditispublishedinthethirdvolumeofthejournalofthatso

cietysirclyellanddrhookerwhobothknewofmyworkthelatterhavingreadmysketcho

fhonouredmebythinkingitadvisabletopublishwithmrwallacesexcellentmemoirso

mebriefextractsfrommymanuscriptsthisabstractwhichinowpublishmustnecessar

ilybeimperfecticannotheregivereferencesandauthoritiesformyseveralstateme

ntsandimusttrusttothereaderreposingsomeconfidenceinmyaccuracynodoubterro

rswillhavecreptinthoughihopeihavealwaysbeencautiousintrustingtogoodautho

ritiesaloneicanheregiveonlythegeneralconclusionsatwhichihavearrivedwitha

fewfactsinillustrationbutwhichihopeinmostcaseswillsufficenoonecanfeelmor

esensiblethanidoofthenecessityofhereafterpublishingindetailallthefactswi

threferencesonwhichmyconclusionshavebeengroundedandihopeinafutureworkto do

this for I am well aware that scarcely a single point is discussed in this volume on which

facts cannot be adduced often apparently leading to conclusions directly

opposite to those at which i have arrived a fair result can be obtained only by fully stating and

balancing the facts and arguments on both sides of each question and this cannot possibly

be here done