Vivek Patel

CSC 440

Assignment 2

1. 1. 18a + b = 3

13a + b = 4

5 a = -1

a = -1 + 5^-1 = -21

a = 5

18\*5 + b = 3 90 + b = 3 12 + b = 29

b = 17

testing: 13\*5 + 17 = 82 (mod 26) = 4

* 1. 21(y -17) = x (mod 26)

x = 21y + 7

* 1. D E J X D I J Y Z

3 4 9 23 3 8 9 24 25

70 91 196 490 70 175 196 511 532

18 13 14 22 18 19 14 17 12

SNOWSTORM

1. There would be no advantage as the new cipher because a1 and a2 ( a from both affine ciphers) would both be prime with 26 as will be their product (a1a2). The decryption key would be the same as if there were only a single affine cipher used to encrypt the text.
2. 1. WINTER = [22 8], [13 19], [4 17]

multiplied with key = [144 198], [185 274], [135 207] mod 26 = [14 16], [3 14], [5 25]

OQDOFZ

* 1. M-1 = (4\*11 – 5 \* 7)^-1 |11 -7| = (44- 35)^-1 = 9^1 = 3

|-5 4|

|11\*3 -7\*3| |33 -21| |7 5|

|-5\*3 4\*3| = |-15 12| = |11 12|

1. The highest confidence key length is 6. The key is “DARWIN” and the text is :

“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 on all sorts of facts which could possibly have any bearing on it after five years work I allowed myself to speculate on the subject and drew up some short notes these I enlarged in into a sketch of the conclusions which then seemed to me probable from that period to the present day I have steadily pursued the same object I hope that I may be excused for entering on these personal details as I give them to show that I have not been hasty in coming to a decision my work is now nearly finished but as it will take me two or three more years to complete it and as my health is far from strong I have been urged to publish this abstract I have more especially been induced to do this as mr Wallace who is now studying the natural history of the malay archipelago has arrived at almost exactly the same general conclusions that I have on the origin of species last year he sent to me a memoir on this subject with a request that I would forward it to sir Charles lyell who sent it to the linnean society and it is published in the third volume of the journal of that society sir clyell and dr hooker who both knew of my work the latter having read my sketch of honoured me by thinking it advisable to publish with mr wallaces excellent memoir some brief extracts from my manuscripts this abstract which I now publish must necessarily be imperfect I cannot here give references and authorities for my several statements and I must trust to the reader reposing some confidence in my accuracy no doubt errors will have crept in though I hope I have always been cautious in trusting o good authorities alone I can here give only the general conclusions at which I have arrived with a few facts in illustration but which I hope in most cases will suffice no one can feel more sensible than i do of the necessity of here after publishing in detail all the facts with references on which my conclusions have been grounded and I hope in a future work to do this for I am well aware that scarcely a single point is discussed in this volume on which facts cannot be adduced of ten 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”

1. Included in zip as Bbsprng.java