Lab 3

Tyler Janvrin

1.1

Letter key:

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

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

1.

A T T A C K A T D A W N

0 19 19 0 2 10 0 19 3 0 22 13  
L E M O N L E M O N L E

11 4 12 14 13 11 4 12 14 13 11 4 ADD THE CIPHERTEXT AND PLAINTEXT

L X F O P V E F R N H R

2.

S S I O E P C A I

L E M O N L E M O

18 18 8 14 4 15 2 0 8 SUBTRACT THE KEY FROM THE CIPHERTEXT

11 4 12 14 13 11 4 12 14

H O W A R E Y O U

3. SUBTRACT THE PLAINTEXT FROM THE CIPHERTEXT

C R Y P T O G R A P H Y

2 17 24 15 19 14 6 17 0 15 7 24

C E E T E O T X E A H L

2 4 4 19 4 14 19 23 4 0 7 11

A N G E P A N G E P A N

The key is ANGEP (is that a word?)

1.2

1.

If he had anything confidential to say, he wrote it in  
cipher, that is, by so changing the order of the letters of  
the alphabet, that not a word could be made out

GUELPH

Oz lp whj urjioohk ndulchpcaoup ed zgs, lp lyuni ti pt

wmawlx, nlli py, vc dd jnurrxum nlp dyjyv zu any ppiaklw zu

any eweogvie, iogn rzi h civo rvafh mt tgxi zja

2.

Xum opee omnunh gpk Hikrvkde gvxnqr, pvsk mlp bbnqr  
tbtemltuihqtmp kobhiea, oe ts qqysumfm zte tyioztikb rqtxrz  
ldeuhmtoy xb qtfevsmxq wmgp g etvnqmttjbzcmrh nxvxignboan ss  
nxqqyrvik arnteeiw. Swx unwgitoe, ms X oe tlr uuet jemwgerg  
tkftie qt m cmcpkdtikb ctowr xrmirgmdf iw vv Kzgpvan, ani  
zqmtt whavqcx gpgf P gbzxqstbvje ts R aozci R qy fhi zwyf  
fvryaqnxyg aeeh ymzfev vv Kzgpvan.

ENIGMA

The idea behind the Vigenere cipher, like all other

polyalphabetic ciphers, is to disguise the plaintext letter

frequency to interfere with a straightforward application of

frequency analysis. For instance, if P is the most frequent

letter in a ciphertext whose plaintext is in English, one

might suspect that P corresponds to E since E is the most

frequently used letter in English.

2 – Playfair Cipher

2.1

Key: Gracefully Kept

Phrase: Balloons Paradise

BA LX LO ON SP AR AD IS EX

NL YW YN QO GI CA CB SG EY

Decode the ciphertext

PQ YW BL CU YN VP UG NX OW

HI LX LA RY LO ST FR OW NX

2.2

BL RB GS AL SD PA UL LI RL ID GV

AR EA LX LR IG HT SR ES ER VE DX

Are all rights reserved

2.3

EY DL AF LX HD TS XL YD AT ST IQ HU BI MW PS TC BI PN KO BZ WE ZB LB QF YM RZ LZ MY WB ZB EA CB FM OI PE FP PN OP CP BI FB IZ IB BL NB VS QZ BL ZE PY FQ MD OI PE FP

// this doesn’t look right, but I did it twice and couldn’t find anything wrong with it

HE LX LO HA PX PY FE ET

BD NQ MP KD NZ OZ BR DI