BEGIN CIPHER MANUAL

This system relies on the use of an alphanumeric key comprised of two parts in addition to a 6x6 grid.

1 Key Requirements

- The first part of the key may contain numbers and letters and must be 2 or more characters. It will be referred to as the "key-word".
- The second part of the key is a 3 digit number, consisting solely of distinct digits from the set {1,2,3,4,5,6}. It will be referred to as the "key-number".
- The two keys are presented in the form EXAMPLE 123 to make sure the key-number is not confused with a trailing digit of the key-word.
- **NOTE: 'Y' is assumed to be a vowel for this cipher.**

2 Encryption

A fully worked example is provided below using the key `KRYPTOS 456` and the plaintext `abcde fghij klmno pqrst uvwxy z`.

2.1 Creating the 6x6 grid

Similar to the Playfair cipher, the key-word is streamed in left to right, top to bottom removing any letters that may appear twice. The remaining unused characters are then streamed in. The plain alphabet to be used is numeric digits 0 through 9 followed by the standard Roman alphabet in alphabetical order.

Using the key-word, we obtain the grid below.

K	R	Y	P	T	O
S	0	1	2	3	4
5	6	7	8	9	A
B	C	D	E	F	G
H	I	J	L	M	N
Q	U	V	W	X	Z

The key-number is a a permutation of the columns in the grid formed above. Thus `456` is read as "column 4 goes to column 5, column 5 goes to column 6, and column 6 goes to column 4." The updated grid is shown below.

K	R	Y	O	P	T
S	0	1	4	2	3
5	6	7	A	8	9
B	C	D	G	E	F
H	I	J	N	L	M
Q	U	V	Z	W	X

2.2 Partitioning the plaintext

The plaintext will then be partitioned into repeating 1, 2, and 3 character groups depending on certain characteristics of the key-word.

- first n-gram length
  - if the length of the key-word is prime, the first number is 1
  - else if the length of the key-word is even, the first number is 2
  - else if the length of the key-word is odd, the first number is 3
- second n-gram length
  - if second character of the key-word is a consonant, the second number is the maximum of the remaining numbers
  - if second character of the key-word is a vowel or number, the second number is the minimum of the remaining numbers
- third n-gram length
  - the only remaining number

Example key-words and their corresponding partition sizes are shown below.

- ANT generates 1 3 2
- CAT generates 1 2 3
- OWLS generates 2 3 1
- DOGS generates 2 1 3
- ABANDONER generates 3 2 1
- EAGLEWOOD generates 3 1 2

With a length 7 and first character being a consonant, `KRYPTOS` would partition the text into repeating 1, 3, and 2 length n-grams. Our plain text would now appear as `a bcd ef g hij kl m nop qr s tuv wx y z01 23 4 567 89`.

NOTE: continue partitioning text until the length of the remaining characters is less than or equal to the next sized partition to be used. Further, make sure to pad all double letters that appear, regardless of partition, with the letter 'x'. If a double 'x' appears, pad with the letter 'z'.

2.3 Applying grid to partitioned text

The following rules will be used to encrypt the newly created partitions.

- For 1-grams, choose the character that is symmetric across the main diagonal. If the character already appears on the main diagonal, choose the character symmetric across the minor diagonal.
- For 2-grams
  - if two characters appear in the same row, shift each one character to the right, cycling around to the left if needed
  - if two characters appear in the same column, shift each one character down, cycling around to the top if needed
  - if two characters are in different rows and columns, draw a rectangle around them and choose the characters in the corners and in the same row as the plain letter.
- For 3-grams, for each letter, locate the 2x2 sub-square it is located in, and replace with the character diagonally across in the sub-square.

Applying these rules to the partitioned plaintext, we find the ciphertext to be `D 65A FB 7 UQZ PH W V13 UK R 2HN XQ 5 JKO 3S C CBG 95`.

3 Decryption

To decrypt a given ciphertext, use the same instructions provided in **2.1** and **2.2** to create the grid and partition the ciphertext appropriately.

The inverse rules of section **2.3** are provided below.

- For 1-grams, choose the character that is symmetric across the main diagonal. If the character already appears on the main diagonal, choose the character symmetric across the minor diagonal.
- For 2-grams
  - if two characters appear in the same row, shift each one character to the left, cycling around to the right if needed
  - if two characters appear in the same column, shift each one character up, cycling around to the bottom if needed
  - if two characters are in different rows and columns, draw a rectangle around them and choose the characters in the corners and in the same row as the plain letter.
- For 3-grams, for each letter, locate the 2x2 sub-square it is located in, and replace with the character diagonally across in the sub-square.

END CIPHER MANUAL[1]

[1] Both Spencer Anderson and Ethan Battaglia have confirmed the practicality and consistency of the cipher system outlined above.

BEGIN INSTRUCTOR COPY

Key 1

The first key used is `MADELINEDOROTHY 513`.

Below is the 6x6 grid with the key-word (left) and the permuted grid (right).

M	A	D	E	L	I
N	O	R	T	H	Y
0	1	2	3	4	5
6	7	8	9	B	C
F	G	J	K	P	Q
S	U	V	W	X	Z

L	A	M	E	D	I
H	O	N	T	R	Y
4	1	0	3	2	5
B	7	6	9	8	C
P	G	F	K	J	Q
X	U	S	W	V	Z

With key-word length 15 and second letter 'A', the partition sizes are `3 1 2`.

Partitioned text: `abc d ef ghi j kl mno p qr stu v wx yz0 1 23 456 7 89`.

Ciphertext: `H12 P MK XAR O PE TEL D JY KMP Q VU DJ9 N 52 783 T C8`.

Re-partitioned ciphertext: `H12PM KXARO PETEL DJYKM PQVUD J9N52 783TC 8`.

Key 2

The second key used is `DIMITRAREAGAN 614`.

Below is the 6x6 grid with the key-word (left) and the permuted grid (right).

D	I	M	T	R	A
E	G	N	0	1	2
3	4	5	6	7	8
9	B	C	F	H	J
K	L	O	P	Q	S
U	V	W	X	Y	Z

A	I	M	D	R	T
2	G	N	E	1	0
8	4	5	3	7	6
J	B	C	9	H	F
S	L	O	K	Q	P
Z	V	W	U	Y	X

With key-word length 13 and second letter 'I', the partition sizes are `1 2 3`.

Partitioned text: `i 24 am3 5 th e0x 0 7w alr u sa xab x by ank e xe dox o dl e9x 9 8x 8`.

Ciphertext: `2 G8 GEC 9 RF MRQ V 5Y GZO F Z2 QG8 A HV GDW B UO NUQ 7 IK M5Q 5 6Z M.`

Re-partitioned ciphertext: `2G8GE C9RFM RQV5Y GZOFZ 2QG8A HVGDW BUONU Q7IKM 5Q56Z M`.

Key 3

The third key used is `XYLOPHONEJACUZZI 452`.

Below is the 6x6 grid with the key-word (left) and the permuted grid (right).

X	Y	L	O	P	H
N	E	J	A	C	U
Z	I	0	1	2	3
4	5	6	7	8	9
B	D	F	G	K	M
Q	R	S	T	V	W

X	P	L	Y	O	H
N	C	J	E	A	U
Z	2	0	I	1	3
4	8	6	5	7	9
B	K	F	D	G	M
Q	V	S	R	T	W

With key-word length 16 and second letter 'Y', the partition sizes are `2 1 3`.

For the plaintext we chose an excerpt from *Angle Side Angle*, a short story from the Winter 2010 copy of the Whistling Shade journal. You might be familiar with it.

Partitioned text: `tw o min ut e sbe fo r eth eb e lxl mr s jen se n was xs t ilx lp o und in g xge om e try pr o xof so n the bl a ckb oa r dye lx l owc ha l kdu st c ake dh e rfi ng e rti ps a nds pe c kle dh e rbl ac k hai ri t was fr i day an d non eo f the ot h erk id s car ed a bou th e rth eo r ems an d pos tu l ate sb u tsh ew a sun nf a zed.`

Ciphertext: `WQ B T6P AW 8 DVL GL 9 LMA ND 8 ECE DW 3 YLP RJ P GHD LQ M 6EC YL B OPS ZE C CWL HG 8 MFJ YV B CUR TL P MAL FX K XQV A1 9 SJL YP Z UGX OU Z QSO RW G HQL MY 8 FR6 AB 8 FM6 LV K PSD YC G QEL MY 8 FVE UJ A AH6 Y5 M GHD DS 6 SHJ UC 7 PUP AY 1 MAL AO Q LFQ 5R 3 XHF IR K VUO WO 8 FMA AY 9 LTD UC 7 NUD WA Z HML QF V MDA UR K DOP JB K 8LS.`

Re-partitioned ciphertext: `WQBT6 PAW8D VLGL9 LMAND 8ECED W3YLP RJPGH DLQM6 ECYLB OPSZE CCWLH G8MFJ YVBCU RTLPM ALFXK XQVA1 9SJLY PZUGX OUZQS ORWGH QLMY8 FR6AB 8FM6L VKPSD YCGQE LMY8F VEUJA AH6Y5 MGHDD S6SHJ UC7PU PAY1M ALAOQ LFQ5R 3XHFI RKVUO WO8FM AAY9L TDUC7 NUDWA ZHMLQ FVMDA URKDO PJBK8 LS.`

END INSTRUCTOR COPY[2]

[2]Both Spencer Anderson and Ethan Battaglia have confirmed the accuracy of the ciphertexts encrypted above.

B3G1N 5TUD3NT C0PY

enrypted ciphrtext numbre two

2G8GE C9RFM RQV5Y GZ0FZ 2QG8A HVGDW BU0NU Q7IKM 5Q56Z M

encyrpted cihprtext nomber one

H12PM KXARO PETEL DJYKM PQVUD J9N52 783TC 8

ernypted ciphertеext nunber three

WQBT6 PAW8D VLGL9 LMAND 8ECED W3YLP RJPGH DLQM6 ECYLB OPSZE
CCWLH G8MFJ YVBCU RTLPM ALFXK XQVA1 9SJLY PZUGX OUZQS ORWGH
QLMY8 FR6AB 8FM6L VKPSD YCGQE LMY8F VEUJA AH6Y5 MGHDD S6SHJ
UC7PU PAY1M ALAOQ LFQ5R 3XHFI RKVUO WO8FM AAY9L TDUC7 NUDWA
ZHMLQ FVMDA URKDO PJBK8 LS

3ND 5TUD3NT C0PY[3]

[3]Good luck :)