Worksheet 19 (Cryptography 3): Sophisticated Hand Ciphers

Group Names: ______________________________

Transposition ciphers are vulnerable to frequency analysis, and shift ciphers are easy to break. This worksheet introduces some more sophisticated ciphers that still are easy enough to encode and decode without computers, and that can rely on fairly short keys for their security.

The first two ciphers are example of *polyalphabetic ciphers*, which use different encoding schemes for different letters in the plaintext.

To encrypt and decrypt ciphers that rely on multiple shift ciphers, it is helpful to use a "tabula recta", a grid that contains all the letters of the alphabet along with each shift.

1. Progressive Caesar Cipher (Sequential Shift)

(a) Using a private key of $A \to J$ (and sequential shift), encrypt the word CONSTITUTION.

C O N S T I T U T I O N

L Y Y E G W I K K A H H

(b) Using a private key of $A \to$ ~~C~~ D, decrypt the ciphertext WLJXP OQDZR GVTFV GIFZ

THERIGHTOFTHEPEOPLE

D E F G H I J K L M N O P Q R S T U V

(c) What are some advantages of this cipher?

obscures frequency analysis, double letters

(d) What are some disadvantages of this cipher?

it's easy to lose track of what line you're on

Easy to break if you know what kind of cipher you are decrypting.

2. Vigenère Cipher

(a) Using the keyword UNION, encode the word CONSTITUTION.

C	O	N	S	T	I	T	U	T	I	O	N
U	N	I	O	N	U	N	I	O	N	U	N
W	B	V	G	G	C	G	C	H	V	I	A

(b) Using the keyword UNION, decode the ciphertext VVTZB ZEQUU NF

V	V	T	Z	B	Z	E	Q	U	U	N	F
U	N	I	O	N	U	N	I	O	N	U	N
B	I	L	L	O	F	R	I	G	H	T	S

(c) What are some advantages of this cipher?

Easier to encrypt/decrypt because fewer shifts to remember

Harder to break if you guess one of the shift ciphers correctly.

(d) What are some disadvantages of this cipher?

Bad keywords can lead to the same letter encrypted as the same letter

You can still use repeated pairs in a long enough message + freq. analysis to help you break the cipher.

3. Double Transposition

(a) Use the first keyword RIGHTS and the second keyword UNITE, encrypt the phrase
ESTABLISH JUSTICE

R	I	G	H	T	S
E	S	T	A	B	L
I	S	H	J	U	S
T	I	C	E		

→

G	H	I	R	S	T
T	A	S	E	L	B
H	J	S	I	S	S
C	E	I	T		

Columns → to rows

U	N	I	T	E
T	H	C	A	J
E	S	S	I	E
I	T	L	S	B
S				

→

E	I	N	T	U
J	C	H	A	T
E	S	S	I	E
B	L	T	S	I
				S

JEBCS LHSTA ISTEI S

(b) Assuming the ciphertext was encrypted using double transposition with the first keyword RIGHTS and the second keyword UNITE, decrypt the ciphertext
YESEL INFOE EBSSS BLITR RCUHT EG

27/5 = 5 R 2

27/6 = 4 R 3

E	I	N*	T	U*
Y	I	E	L	C
E	N	B	I	U
S	F	S	T	H
E	O	S	R	T
L	E	S	R	E
		B		G

→

U	N	I	T	E
C	E	I	L	Y
U	B	N	I	E
H	S	F	T	S
T	S	O	R	E
E	S	E	R	L
G	B			

rows → to columns

G*	H	I*	R*	S	T
C	U	E	S	E	R
E	B	H	T	E	L
I	N	S	S	S	G
L	I	F	O	E	B
Y		T	R		

R	I	G	H	T	S
S	E	C	U	R	E
T	H	E	B	L	E
S	S	I	N	G	S
O	F	L	I	B	E
R	T	Y			

(c) What are some advantages of this cipher?

It's quite hard to break

(d) What are some disadvantages of this cipher?

It's tricky to decrypt even when you know the keys, and one transcription error will make it impossible to decrypt.

A *tabula recta.*

To encrypt, find the row with the letter from the key, and the column with the letter you are encrypting; their intersection is the encrypted letter.

To decrypt, find the row with the letter from the key. Then find the letter in that row that you want to decrypt, and then read up that column to find the unencrypted letter at the top.

	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**
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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