25^{th} Annual

Rowan University Programming Contest

hosted by the

Computer Science Department

Friday, 8 April 2011

25^{th} Annual

Rowan University Programming Contest

hosted by the

Computer Science Department

Friday, 8 April 2011

Transposition and Substitution Ciphers

Transposition Cipher

Rearrange the letters by writing the message in rows, and then copy down the columns as new rows in order based on a keyword:

Original (written across)

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

Transposed

C	**H**	**M**	**R**	**W**	← 'A'
E	J	O	T	Y	← 'E'
B	G	L	Q	V	← 'N'
D	I	N	S	X	← 'P'
A	F	K	P	U	← 'S'

Keyword:	S	N	A	P	E
Order:	5	3	1	4	2

The columns become rows, ordered by the letters in the keyword. Thus we get **CHMRWEJOTYBGLQVDINSXAFKPU**.

To decode, reverse the process: make the first row into the column that corresponds with the letter's position in the keyword.

Substitution Cipher

A *Cæsar Cipher* shifts the alphabet by some number of characters. (Letters shifted off one end wrap around to the other.) If you shift by one, then **adept** becomes **befqu**:

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 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

If you shift by three, then **adept** becomes **dghsw**:

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
↓ ↓ ↓ ↓ ↓
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

But this is easy to crack, because each letter is always substituted the same way.

Better Substitution

Substitute as in a Cæsar cipher, except that instead of shifting each letter the same amount, we'll shift based on a keyword, using A=1, B=2, and so on. (Lowercase letters are negative.)

The keyword 'Abe' would have the values {1, -2, -5}. So if we encode 'HELLO WORLD.', we get:

Orig.	H	E	L	L	O	_	W	O	R	L	D	.
Key	A	b	e	A	b		e	A	b	e	A	
Shift	1	-2	-5	1	-2		-5	1	-2	-5	1	
Result	I	C	G	M	L	_	R	N	P	G	E	.

Note that unlike the transposition cipher, we don't process non-alpha characters.

Important Differences

Line Length

If transposing a line with fewer than 25 characters, pad with letters starting at 'A' to fill in the grid.

```
'THIS IS NOT A STEP.'
```

is encoded as

```
'THIS IS NOT A STEP.ABCDEF'
```

Substitution does not care about line length.

Important Differences

Relevant Characters

Transpose **every** character in the 25-character block, including spaces, digits, and punctuation.

Substitute **only the letters**. Non-alphabetical characters are passed unchanged and do not change the current position in the keyword.

Important Differences

Keywords
Transposition keywords are all-uppercase.
Substitition keywords can be mixed case.

A transposition keyword must have at least 5 unique letters. Skip duplicate letters. If there are more than five, ignore the extras. (The keyword 'TELEPHONE' would be treated as 'TELPH'.)

If a transposition keyword does not have at least 5 unique letters, (such as the keyword 'SNOW'), use 'ABCDE' instead.

A substitition keyword can be any length and have repeated letters.

Important Differences

Remembering Position

When transposing, each 25-character block is independent.

When substituting, you must keep track of keyword position from one line to the next. If we had a 2nd line after the example above:

Orig.	H	E	L	L	O	_	W	O	R	L	D	.
Key	A	b	e	A	b		e	A	b	e	A	
Shift	1	-2	-5	1	-2		-5	1	-2	-5	1	
Result	I	C	G	M	L	_	R	N	P	G	E	.

Orig.	T	E	S	T	I	N	G	_	1	2	3
Key	b	e	A	b	e	A	b				
Shift	-2	-5	1	-2	-5	1	-2				
Result	R	Z	T	R	D	O	E	_	1	2	3

Combined Cipher

For this contest, we are going to combine these two ciphers.

First, transpose the characters of a message with the transposition keyword.

Then, substitute *only the letters* with the substitution keyword.

If either keyword is 'PASS', skip that step.

For decoding, reverse the steps: first un-do the substitution, and then un-do the transposition.

Note that any decrypting which involves transposition will have lines of exactly 25 characters, because the lines were padded when they were originally encrypted.

Combined Cipher

Transposing with "HOBAN", substituting with "Washburne":

```
CURSE YOUR SUDDEN BUT
INEVITABLE BETRAYAL!
```

Pad the 1st line out to 25 characters: `CURSE YOUR SUDDEN BUTABCD`

Original (written across)

C	U	R	**S**	E
_	Y	O	**U**	R
_	S	U	**D**	D
E	N	_	**B**	U
T	A	B	**C**	D

Transposed

S	**U**	**D**	**B**	**C**	← 'A'
R	O	U	_	B	← 'B'
C	_	_	E	T	← 'H'
E	R	D	U	D	← 'N'
U	Y	S	N	A	← 'O'

Keyword:	H	O	B	A	N
Order:	3	5	2	1	4

Now: `SUDBCROU_BC__ETERDUDUYSNA`

Combined Cipher

Transposing with "HOBAN", substituting with "Washburne":

Pad the 2nd line out to 25 characters: `INEVITABLE BETRAYAL!ABCDE`

	Original (written across)					Transposed					
	I	N	E	**V**	I	**V**	**L**	**T**	**L**	**D**	← 'A'
	T	A	B	**L**	E	E	B	E	A	C	← 'B'
	_	B	E	**T**	R	I	T	_	A	A	← 'H'
	A	Y	A	**L**	!	I	E	R	!	E	← 'N'
	A	B	C	**D**	E	N	A	B	Y	B	← 'O'
Keyword:	H	O	B	A	N						
Order:	3	5	2	1	4						

Now: `VLTLDEBEACIT_AAIER!ENABYB`

Combined Cipher

Transposing with "HOBAN", substituting with "Washburne":

S	U	D	B	C	R	O	U	_	B	C	_	_	E	T	E	R	D	U	D	U	Y	S	N	A
W	a	s	h	b	u	r	n	_	e	W	_	_	a	s	h	b	u	r	n	e	W	a	s	h
23	-1	-19	-8	-2	-21	-18	-14	_	-5	23	_	_	-1	-19	-8	-2	-21	-18	-14	-5	23	-1	-19	-8
P	T	K	T	A	W	W	G	_	W	Z	_	_	D	A	W	P	I	C	P	P	V	R	U	S

V	L	T	L	D	E	B	E	A	C	I	T	_	A	A	I	E	R	!	E	N	A	B	Y	B
b	u	r	n	e	W	a	s	h	b	u	r	_	n	e	W	a	s	_	h	b	u	r	n	e
-2	-21	-18	-14	-5	23	-1	-19	-8	-2	-21	-18	_	-14	-5	23	-1	-19	_	-8	-2	-21	-18	-14	-5
T	Q	B	X	Y	B	A	L	S	A	N	B	_	M	V	F	D	Y	!	W	L	F	J	K	W

Original Message	Final Result
CURSE_YOUR_SUDDEN_BUT	PTKTAWWG_WZ__DAWPICPPVRUS
INEVITABLE_BETRAYAL!	TQBXYBALSANB_MVFDY!WLFJKW