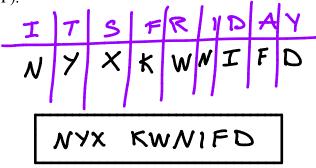**Name:** _Solutions_   score:_____ / 10
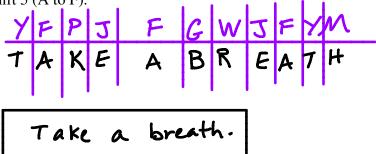
There are 10 points possible on this quiz. No aids (book, notes, etc.) are permitted. You may use a calculator. **Show all work and supporting calculations for full credit. Explain how you get your answers.**

   A tabula recta is available.

1. (2 points) **Encrypt** the message IT'S FRIDAY using an alphabetic Caesar cipher with shift 5 (A to F).
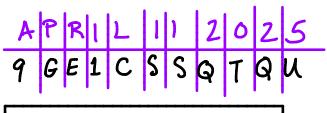
I	T	S	F	R	I	D	A	Y
N	Y	X	K	W	N	I	F	D

   NYX KWNIFD

2. (2 points) **Decrypt** the message YFPJ F GWJFYM using an alphabetic Caesar cipher with shift 5 (A to F).

Y	F	P	J	F	G	W	J	F	Y	M
T	A	K	E	A	B	R	E	A	T	H

   Take a breath.

3. (2 points) **Encrypt** the message APRIL 11 2025 using the substitution table below.

original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
maps to	9	8	7	6	5	4	3	2	1	0	D	C	B	A	H	G	F	E

original	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
maps to	L	K	J	I	P	O	N	M	T	S	Q	R	V	U	Y	X	W	Z

A	P	R	I	L	1	1	2	0	2	5
9	G	E	1	C	S	S	Q	T	Q	U

   9GE1C SS QTQU

4. (2 points) **Encrypt** the message WHICH ONE ARE YOU using a tabular transposition cipher with rows of length 6.

1	2	3	4	5	6
W	H	I	C	H	O
N	E	A	R	E	Y
O	U	X	X	X	X

input to rows

extract columns

cipher text : WNO HEU IAX CRX HEX OYX

5. (3 points) **Decrypt** the message SUHKO GEOUH EXROC XDRHX OCAX using a tabular transposition cipher with rows of length 6.

Code word has 24 letters. Thus $24/6 = 4$ rows.
Input codeword to <u>columns</u> of grid.

1	2	3	4	5	6
S	O	U	R	D	O
U	G	H	O	R	C
H	E	E	C	H	A
K	O	X	X	X	X

→ extract rows

plain text : SOURDOUGH or
CHEECHAKO

6. (1 point) Describe at least one aspect of a Caesar cipher that makes it vulnerable to being hacked (that is, deciphered by an unwanted observer).

- Once a single letter is correclty deciphered, you have the entire key to decryption.
- Frequency analysis can be used to guess particular letters.
- There are only 25 different possibilities so it's easy to check by hand or by computer.