CIS 3362 Quiz #2 Solutions

1) (10 pts) Encrypt the plaintext "ITSTIMEFORTHEWEEKEND" using the Playfair cipher and the keyword "SUMMERTIME". Please use 'X' as the padding character and please use the box provided below to visualize the key.

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

First write out plaintext in pairs: `IT ST IM EF OR TH EW EX EK EN DX`

`AITDAUUHQMBDUYMYRHUPGV`

Grading: 5 pts for the box (1 pt off for each error in keyword fill), 5 pts for the ciphertext, grade proportionally.

2) (3 pts) What is the full set of plaintext characters that could be encrypted by the ADVGVX cipher? (Describe the set. State its size and which characters it contains.)

The plaintext had to be comprised from a set of 36 characters: the 26 letters or 10 digits, so ('A' through 'Z' and '0' through '9'.)

Grading: 1 pt for 36, 1 pt for letters, 1 pt for digits

3) (6 pts) Briefly describe the roles that Hans-Thilo Schmidt and Marian Rejewski played in relation to the Enigma machine/code used by the Germans before and during World War II. (A single sentence for each will suffice.)

Hans-Thilo Schmidt was the German who met the secret French agent "Rex" and allowed Rex to take pictures of the books describing how the Enigma was built.

Marian Rejweski was the Polish mathematician who was instrumental in initially breaking the Enigma in the 1930s.

Grading: 3 pts for each, give partial as you see fit. More details are okay.

4) (8 pts) Describe the details of how the Navajo Code worked, including how Navajo words were used and what they represented. (Credit will be given relatively, based on the level of detail. Quite a bit of class time was spent on this description.)

Any word with a regular Navajo translation was just spoken in Navajo.

Many words without translations that are frequently used in the military were assigned code words in Navajo. These words/terms were things like military positions (commander, general, etc.), military groups (battalion, etc.) countries, aircraft, ships, weapons, even the months.

If there were words that popped up that didn't have a Navajo translation or a pre-assigned code word, then the word would have to be "spelled out." Each letter had a code word in Navajo (for example, the letter 'A' was assigned the Navajo word for ant.) Later, to thwart frequency analysis among the situations where words were spelled out, multiple (about 3) code words were assigned to each letter.

Grading: 3 pts for stating that regular Navajo was usually used.
3 pts for stating that specific military/WWII terms w/o a Navajo translation were assigned code words
2 pts for stating that a method existed to spell out other words that weren't covered by the first two categories

5) (10 pts) The following ciphertext was encrypted using the column permutation cipher (transposition) with the keyword "RECORD". What is the corresponding plaintext? (Hint: The answer is a regular message in English.)

ULOEEEWDVSLHHOKOACTTVDNHMMDSAEYETEEAOEAOPTTGE

Note: There are 45 characters in the ciphertext. The grid is set up below to help you. It is recommended that you put the keyword on row 1, and integers 1 through 6 in row 2, and then copy the ciphertext into the grid (in some order…)

R	E	C	O	R	D
5	3	1	4	6	2
Y	O	U	H	A	V
E	A	L	M	O	S
T	C	O	M	P	L
E	T	E	D	T	H
E	T	E	S	T	H
A	V	E	A	G	O
O	D	W	E	E	K
E	N	D			

Since the ciphertext is 45 characters long, the short columns have 45/6 = 7 characters, and there are 45%6 = 3 long columns (these are columns labeled 5, 3 and 1, respectively.) The long columns have 8 characters. Thus, since the column labeled 1 is the third one, we will read the first eight

characters of the ciphertext into this column, going down. The column labeled 2 is the sixth one, so we'll read the next 7 characters from top to bottom into this column. Continue in this fashion. When we read in the third and fifth set of letters, we'll read 8 letters down the column again.

Now, read the message starting at the top row:

YOU HAVE ALMOST COMPLETED THE TEST. HAVE A GOOD WEEKEND!

Grading: full credit it correct. If it's not correct, give partial as follows:
1 pt – writing down keyword at top
2 pts – correctly labeling ordering based on keyword
3 pts – some sort of evidence of copy data down by columns (and not rows)
3 pts – if you feel more partial credit is deserved (though I don't think this will come up much)

6) (12 pts) The ciphertext from the Hill cipher is "IAJL". The **encryption** key is $\begin{pmatrix} 6 & 9 \\ 3 & 7 \end{pmatrix}$. What is the original plaintext? (Hint: The answer is a normal English word. If you don't get a word you recognized, you did something wrong.)

First, we must get the decryption key using the formula from class:

$$(6 \times 7 - 3 \times 9)^{-1} (mod\ 26) \begin{pmatrix} 7 & -9 \\ -3 & 6 \end{pmatrix} = 15^{-1} (mod 26) \begin{pmatrix} 7 & -9 \\ -3 & 6 \end{pmatrix} = \begin{pmatrix} 7 \times 7 & -9 \times 7 \\ -3 \times 7 & 6 \times 7 \end{pmatrix}$$

Now, map these values mod 26, to equivalent values mod 26 that will be easy to do arithmetic with:

$$\begin{pmatrix} -3 & -11 \\ 5 & -10 \end{pmatrix}$$

Now, decrypt both pairs of letters:

$\begin{pmatrix} -3 & -11 \\ 5 & -10 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix} = \begin{pmatrix} -24 \\ 40 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix}$, thus the first two letters of plaintext are "CO"

$\begin{pmatrix} -3 & -11 \\ 5 & -10 \end{pmatrix} \begin{pmatrix} 9 \\ 11 \end{pmatrix} = \begin{pmatrix} -27 - 121 \\ 45 - 110 \end{pmatrix} \equiv \begin{pmatrix} -148 \\ -65 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 13 \end{pmatrix}$, thus the next 2 letters are "IN".

The corresponding plaintext is **COIN.**

Grading: 1 pt 15^{-1},
1 pt each entry in matrix (4 pts),
1 pt for $15^{-1} = 7$,
2 pts to simplify decryption key (doesn't have to be 0 to 25…).
2 pts – extracting first pair
2 pts – extracting second pair

7) (1 pt) In which city did the WWII Battle of Berlin occur? **Berlin (Give to All)**