Homework #3A Solutions - CIS 3362

1) (10 pts) By hand, encrypt the plaintext "HELLOBYRONLOVELYDAY" with the keyword "BUILDINGBLOCK" and the padding character "Q".

. . . . . .

In order to encrypt this plaintext with Playfair, we must create the key.

Step 1: Start with an empty 5x5 grid:

Start filling in the grid using the keyword "BUILDINGBLOCK", skipping over letters already in the grid and combining I/J into a single cell:

B	U	I/J	L	D
N	G	O	C	K

Fill in the rest of the grid with characters not used in the keyword, in alphabetical order:

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

Step 2: Break apart the plaintext into blocks of 2 characters, adding the padding character "Q" whenever a block has 2 of the same character:

HE L**Q** LO BY RO NL OV EL YD AY

Using the 3 rules of the Playfair cipher, encrypt each 2-character block by finding their location in the grid. These rules are:

1) Same Row - Move right by 1 space with wraparound
2) Same Column - Move down by 1 space with wraparound
3) Different Row/Column - Box rule: Treat the characters as corners of a "box" and encrypt each character as the other corner of the box **on the same row**

The following are some examples of encryption based on each rule:

Encrypting HE:

B	U	I/J	L	D		B	U	I/J	L	D
N	G	O	C	K		N	G	O	C	K
A	$\mathbf{E}_2$	F	$\mathbf{H}_1$	M	$\Rightarrow$	A	E	$\mathbf{F}_2$	H	$\mathbf{M}_1$
P	Q	R	S	T		P	Q	R	S	T
V	W	X	Y	Z		V	W	X	Y	Z

Encrypting LQ:

B	U	I/J	$\mathbf{L}_1$	D		B	$\mathbf{U}_1$	I/J	L	D
N	G	O	C	K		N	G	O	C	K
A	E	F	H	M	$\Rightarrow$	A	E	F	H	M
P	$\mathbf{Q}_2$	R	S	T		P	Q	R	$\mathbf{S}_2$	T
V	W	X	Y	Z		V	W	X	Y	Z

Encrypting RO:

B	U	I/J	L	D		B	U	I/J	L	D
N	G	$\mathbf{O}_2$	C	K		N	G	O	C	K
A	E	F	H	M	$\Rightarrow$	A	E	$\mathbf{F}_2$	H	M
P	Q	$\mathbf{R}_1$	S	T		P	Q	R	S	T
V	W	X	Y	Z		V	W	$\mathbf{X}_1$	Y	Z

HE LQ LO BY RO NL OV EL YD AY

\- -

MF US IC LV XF CB NX HU ZL HV

Ciphertext: MFUSICLVXFCBNXHUZLHV

---

2) (10 pts) Show the result of encrypting the plaintext:

"THEQUICKBROWNFOXJUMPEDOVERTHE345679INSECTSIN2018"

Using the ADFGVX cipher with the 6x6 square shown below and the keyword "SPONGE".

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

. . . . . .

Step 1: Substitution - Substitute each letter in the plaintext with its corresponding 2-letter lookup in the ADFGVX square (go by row-column).

```
T  H  E  Q  U  I  C  K  B  R  O  W  N  F  O  X  J  U  M  P  E  D  O  V  E  R
GD DD AA VF AD AG XG DV XA AF DA DF FD GX DA GG VV AD GV AV AA DG DA FX AA AF

T  H  E  3  4  5  6  7  9  I  N  S  E  C  T  S  I  N  2  0  1  8
GD DD AA XF VX FF FV VA VG AG FD XX AA XG GD XX AG FD FA FG XV AX
```

After substitution: GDDDAAVFADAGXGDVXAAFDADFFDGXDAGGVVADGVAVAADGDAFX-AAAFGDDDAAXFVXFFFVVAVGAGFDXXAAXGGDXXAGFDFAFGXVAX

Step 2: Transposition - Transpose the above ciphertext using the keyword "SPONGE" and the permutation it creates with the alphabetical ordering of its letters:

```
6 5 4 3 2 1
S P O N G E
- - - - - - - - - -
G D D D A A
V F A D A G
X G D V X A
A F D A D F
F D G X D A
G G V V A D
G V A V A A
D G D A F X
A A A F G D
D D A A X F
V X F F F V
V A V G A G
F D X X A A
X G G D X X
A G F D F A
F G X V A X
```

Read down the columns from the keyword in alphabetical order from the keyword "SPONGE" to get the final ciphertext.

Ciphertext: AGAFADAXDFVGAXAXAAXDDAAFGXFAAXFADDVAXVVAFAFGXD-DVDADDGVADAAFVXGFXDFGFDGVGADXADGGGGVXAFGGDADVVFXAF

---

3) (10 pts) For the Hill Cipher, the encryption key is $\begin{pmatrix} 19 & 16 \\ 14 & 3 \end{pmatrix}$, what is the corresponding decryption key? (Assume an alphabet size of 26)

. . . . . .

As the decryption key for the Hill Cipher is simply the inverse of its encryption key matrix, we can apply the matrix inverse formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{26}$$

in order to find the corresponding decryption key:

$$\begin{pmatrix}19 & 16\\14 & 3\end{pmatrix}^{-1} = (19*3-14*16)^{-1} * \begin{pmatrix}3 & -16\\-14 & 19\end{pmatrix} = (-167)^{-1} * \begin{pmatrix}3 & 10\\12 & 19\end{pmatrix}$$

$$= (15)^{-1} * \begin{pmatrix}3 & 10\\12 & 19\end{pmatrix} = 7 * \begin{pmatrix}3 & 10\\12 & 19\end{pmatrix} = \begin{pmatrix}21 & 70\\84 & 133\end{pmatrix} = \begin{pmatrix}21 & 18\\6 & 3\end{pmatrix} \pmod{26}$$

Decryption key: $\begin{pmatrix}21 & 18\\6 & 3\end{pmatrix}$

---

4) (10 pts) You've intercepted a message encrypted by the Hill cipher using a 2x2 key (alphabet size 26). You also know that the plaintext "TR" maps to the ciphertext "UR" and that the plaintext "AP" maps to the ciphertext "BX". What are the possible encryption keys?

. . . . . .

In order to find the possible encryption keys, we must set up a system of equations using the information given above:

$$\begin{pmatrix}\mathbf{T}\\\mathbf{R}\end{pmatrix} \Rightarrow \begin{pmatrix}\mathbf{U}\\\mathbf{R}\end{pmatrix} \qquad \begin{pmatrix}\mathbf{A}\\\mathbf{P}\end{pmatrix} \Rightarrow \begin{pmatrix}\mathbf{B}\\\mathbf{X}\end{pmatrix}$$

$$\begin{pmatrix}19\\17\end{pmatrix} \Rightarrow \begin{pmatrix}20\\17\end{pmatrix} \qquad \begin{pmatrix}0\\15\end{pmatrix} \Rightarrow \begin{pmatrix}1\\23\end{pmatrix}$$

$$\begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}19\\17\end{pmatrix} = \begin{pmatrix}19a+17b\\19c+17d\end{pmatrix} = \begin{pmatrix}20\\17\end{pmatrix} \qquad \begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}0\\15\end{pmatrix} = \begin{pmatrix}15b\\15d\end{pmatrix} = \begin{pmatrix}1\\23\end{pmatrix}$$

$19a + 17b = 20$ $\qquad$ $15b = 1$

$19c + 17d = 17$ $\qquad$ $15d = 23$

Now that we have our system of equations, we can begin solving for the values of a, b, c, and d:

Solving for b:

$15b = 1$
$b = 1 * 15^{-1} \pmod{26}$
$b = 1 * 7$
$b = 7$

Solving for d:

$15d = 23$
$d = 23 * 15^{-1} \pmod{26}$
$d = 23 * 7$
$d = 161$
$d = 5 \pmod{26}$

Solving for a:

$19a + 17b = 20$
$19a + 17(7) = 20$
$19a = 20 - 17(7)$
$19a = -99$
$19a = 5 \pmod{26}$
$a = 5 * 19^{-1} \pmod{26}$
$a = 5 * 11$
$a = 55$
$a = 3 \pmod{26}$

Solving for c:

$19c + 17d = 17$
$19c + 17(5) = 17$
$19c = 17 - 17(5)$
$19c = -68$
$19c = 10 \pmod{26}$
$c = 10 * 19^{-1} \pmod{26}$
$c = 10 * 11$
$c = 110$
$c = 6 \pmod{26}$

Encryption key: $\begin{pmatrix} 3 & 7 \\ 6 & 5 \end{pmatrix}$

5) (10 pts) The Enigma never allowed a character to encrypt to itself. If we consider an arbitrary substitution cipher for an alphabet of 5 letters, we know there are 5! = 120 possible keys. Of these 120 possible keys, how many of them map each plaintext letter to a different ciphertext letter?

. . . . . .

Let's assume our five letters are 'A' through 'E'. The substitution for 'A' can not be 'A'. Without loss of generality, let this substitution be 'B'. If we can count how many permutations have this mapping, we can take that answer and multiply by 4 to get the final answer, since the answer will be the same no matter whether we map A to B, or C, or D or E. Once we map 'A' to 'B', we must map the inputs 'B' through 'E' to the set 'A','C','D','E'. Let's list out all the possible answers that are valid (note, in this list, the first item is what B maps to, the second what C maps to, and so on.) This these in alphabetical order to make sure none are missed.

1. ADEC
2. AECD
3. CAED
4. CDEA
5. CEAD
6. DAEC
7. DEAC
8. DECA
9. EACD
10. EDAC
11. EDCA

It follows that there are 4 x 11 = 44 possible keys that don't map a letter to itself.

Another way to view this problem is as follows:

All permutations can be viewed as cycle chains (as taught in the Enigma lecture). If a letter encrypts to itself, it has a cycle of length 1. Thus, we are being asked to count the number of permutations of 5 items that do NOT have as cycle length of 1.

In order not to have a cycle length of one, have two possibilities:

(a) One cycle of length 2, another of length 3, or
(b) One cycle of length 5.

For (a), we can pick the two items in the cycle of length 2 in 10 ways, since there are 10 ways to choose 2 items out of 5. Once we choose these two items, they swap values. The remaining 3 items can be arranged in a cycle in one of two ways. (If there are three items, A, B and C, then A must map to B or C and the rest of the mappings are fixed.) Thus, there are 10 x 2 = 20 permutations of 5 items which induce cycles of length 2 and 3.

For (b), we arbitrarily choose A as our starting point. There are 4 choices for which letter A maps to. Whatever letter that is, there are 3 choices for the letter that it maps to. Then 2 choices, then one. (Basically, the number of cyclic permutations of n items is always (n-1)! by this logic. Thus, there are 4 x 3 x 2 x 1 = 24 permutations which induce cycles of length 5. Adding, we get 20 + 24 = 44 total permutations.

A final, and more traditional approach (which you can easily find online) to solve the problem is as follows:

A permutation where no item maps to itself is known as a derangement. In popular literature, the problem is posed as follows: if n people come to a party with hats on, and they all want to exchange hats such that no person receives the hat they originally wore to the party, how many ways can they do so? The answer to this question is known as !n. We can prove a recursive formula for !n as follows:

Imagine that we have our n people, and let's consider the case of person 1. Person 1 must receive some one else's hat, let's say person P. We have two cases about person P: either he receives person 1's hat, or someone else's hat.

If person 1 and person P exchange hats, then we are left solving the problem for the n-2 remaining people, which can be done in !(n-2) ways. Notice that there are n-1 choices for person P, so we can do this option in $(n-1)\times!(n-2)$ ways.

If person P receives a hat that is NOT person 1's hat, then if we ignore person 1, there are n-1 people each who must receive n-1 hats, with exactly one banned hat. (Note, person P's banned hat is hat 1. For everyone else, their banned hat is their own.) Since there are n-1 choices for person P, it follows that there are $(n-1)\times!(n-1)$ ways we can do this option.

Putting this together, we have $!n = (n-1)\times(!(n-1)+!(n-2))$. The initial conditions are $!0 = 1$, $!1 = 0$. We find that $!2 = 1$ and $!3 = 2$. $!4 = 3(2+1) = 9$, and $!5 = 4(9+2) = 44$, as desired.