MATH 178 Homework #1

Tamir Enkhjargal

April 2019

HIST

1.

Encrypt the following message. Playfair cipher system, key `SUBHARMONIC`.

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

Putting in our plaintext now:

$$\begin{align}
CH \to FS &\qquad \textit{Corners} \tag{1}\\
RI \to MR &\qquad \textit{Same Row} \tag{2}\\
ST \to AK &\qquad \textit{Corners} \tag{3}\\
IA \to GI &\qquad \textit{Same Column} \tag{4}\\
NS \to RH &\qquad \textit{Corners} \tag{5}
\end{align}$$

Therefore, our ciphertext is now `FSMRAKGIRH`

2.

Decrypt the following message. Playfair cipher system, key `FACETIOUSLY`, ciphertext: `HQSMLFTO`.

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

Decrypting our ciphertext now:

$$\begin{align}
HQ \to LH &\qquad \textit{Same Column} \tag{1}\\
SM \to OP &\qquad \textit{Corners} \tag{2}\\
LF \to IT &\qquad \textit{Corners} \tag{3}\\
TO \to AL &\qquad \textit{Corners} \tag{4}
\end{align}$$

Therefore, our plaintext was `LHOPITAL`.

3.

Decrypt the following message. ADFGVX ciphersystem, key permutation (starts with *zero*): `0L9FN2 TD3OPG HI1ZQC VARE45 XYUMSW 6B8K7J`, keyword: `CREAMY`, ciphertext: `FDDDFVDGVFXDVAFVAGXFGVDV`.

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

Now using our keyword we can layer the keyword, number the letters of the key, and then write the message column by column.

C	R	E	A	M	Y
2	5	3	1	4	6
F	A	V	F	V	G
V	G	F	D	A	V
D	X	X	D	F	D
G	F	D	D	V	V

Now we can use the ADFGVX table to reverse the coordinates we see:

$$FA \quad VF \quad VG \rightarrow H\ U\ M \tag{1}$$

$$VG \quad FD \quad AV \rightarrow M\ I\ N \tag{2}$$

$$DX \quad XD \quad FD \rightarrow G\ B\ I \tag{3}$$

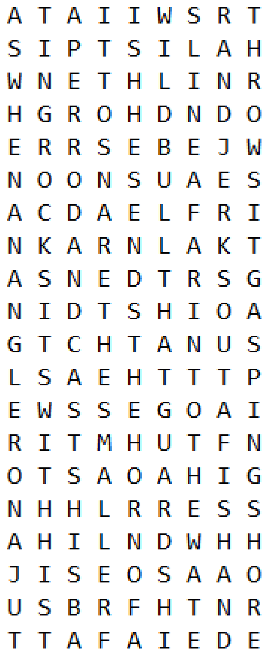
$$GF \quad DD \quad VV \rightarrow R\ D\ S \tag{4}$$

Our plaintext was `HUMMINGBIRDS` then.

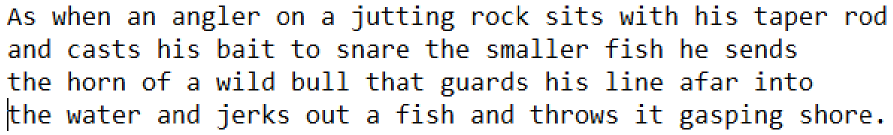
4.

You are an ancient Greek and you intercept a thin strip of paper with the following letters. Decrypt the message. Ciphertext: `ATAIIWSRTSIPTSILAHWNET HLINRHGROHDNDOERRSEBEJWNOONSUAESACDAELFRINKARNLAKTASNEDTRSGNIDTSHIOAGTCHTANUSL SAEHTTTPEWSSEGOAIRITMHUTFNOTSAOAHIGNHHLRRESSAHILNDWHHJISEOSAAOUSBRFHTNRTTAFA`

Cryptanalysis for this one will require factoring the amount of characters there are in this message. There are 180 characters in the ciphertext, and assuming a perfect wrap (no blank characters on the end of the roll), this message can be broken into a message of size: $2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90$. This one took a little bit of handwritten bruteforcing. Just using Notepad, I divided the message into these various sizes and checked if reading down the column made any legible sense.



```
A T A I I W S R T
S I P T S I L A H
W N E T H L I N R
H G R O H D N D O
E R R S E B E J W
N O O N S U A E S
A C D A E L F R I
N K A R N L A K T
A S N E D T R S G
N I D T S H I O A
G T C H T A N U S
L S A E H T T T P
E W S S E G O A I
R I T M H U T F N
O T S A O A H I G
N H H L R R E S S
A H I L N D W H H
J I S E O S A A O
U S B R F H T N R
T T A F A I E D E
```



```
As when an angler on a jutting rock sits with his taper rod
and casts his bait to snare the smaller fish he sends
the horn of a wild bull that guards his line afar into
the water and jerks out a fish and throws it gasping shore.
```

I found that dividing the text into a size of 9 characters worked, and I was able to write out the message by reading down the column. Just as a note, dividing the message into 20 character columns would have also worked, since 9*20=180.

NT

1.

Find gcd(720, 450)

1. Using the Euclidean algorithm

$$\begin{aligned} 720 &= 1 * 450 + 270 && (1)\\ 450 &= 1 * 270 + 180 && (2)\\ 270 &= 1 * 180 + 90 && (3)\\ 180 &= 2 * 90 + 0 && (4) \end{aligned}$$

   The gcd is 90.

2. By factoring each.

$$\begin{aligned} 720 &= 2^4 * 3^2 * 5^1 && (1)\\ 450 &= 2^1 * 3^2 * 5^2 && (2)\\ \therefore gcd &= 2^1 * 3^2 * 5^1 && (3)\\ gcd &= 90 && (4) \end{aligned}$$

2.

For each of the following pairs of numbers, find the gcd using the Euclidean algorithm and then write the gcd as an integer linear combination of the pair:

1. gcd(21, 30)

$$\begin{aligned} 30 &= 1 * 21 + 9 && (1)\\ 21 &= 2 * 9 + 3 && (2)\\ 9 &= 3 * 3 + 0 && (3) \end{aligned}$$

$$\begin{aligned} 3 &= 21 - 2 * 9 && \textit{Start with gcd} && (4)\\ 3 &= 21 - 2(30 - 1 * 21) && \textit{Expand lower value} && (5)\\ 3 &= 3 * 21 - 30 * 2 && \textit{Combine like terms} && (6) \end{aligned}$$

2. gcd(126, 129)

$$\begin{aligned} 129 &= 1 * 126 + 3 && (1)\\ 3 &= 42 * 3 + 0 && (2) \end{aligned}$$

$$3 = -1 * 126 + 1 * 129 \qquad \textit{Start with gcd} \qquad (3)$$

Crypto Challenge

The following is ciphertext from the Vigenere cipher.

```
ptugycymhzgvvzvfxklzgypvjhzlsdsmyckvxvvvatzewfxzldoglzvfrmvzrtfqffgprxhalaycelwtvhvpnc
oshwwelmehhjlmfvojfffhwjogksmfavqvfhvqnolalvtbywkhhlrkskdlzzxdezhbukwckalvfxzxk
cvvqvwgalvfxdejdelrkmhmxzaxastcgaiddehxvhalwyowvajowceeqbukrqkvwjhalxzzxzekha
lfrgxvjkvxhpkokyezzpoiekxmmigmhviwolhkvxueifhdswhalechxyvrwejsmsklhfbefejatspgck
amfbhmxysmymrbzcprfmppvgtuhsmmoivbwvjdolzecahzxkvxlrkwklxiwtukcsphwzbloeucpdlvbbhwbswtc
jsemhzrmoijvtksnqhciivtsjkvxhvvoboeubmzxmrblhrbrmsiatskvcflximrlxsjmpjzuoyiu
```

Using the Kasiski test to determine the key size, the highest likelihood was 5. Using a statistical attack, the key was guessed to be `OTHER`. (resources used from https://www.dcode.fr/vigenere-cipher).

```
BANCHOFFDISCOVEREDHISFIRSTGEOMETRYTHEOREMASAFRESHMANEVERYFRIDAYMORNING...
```