Math 400 Fall 2017
Cryptology HW 1 Solutions
Due Thursday, September 7

1. Encrypt the plaintext message "GO HANG A SALAMI" using a Caesar cipher with a shift (to the right) of 7.

   Solution: "NV OHUN H ZHSHTP"

2. The following ciphertext has been encrypted with a Caesar cipher (with an unknown-to-you shift). Decrypt the message.

   XBPAPHPVCPWDV

   Solution: The shift is fifteen. The plaintext is "IMALASAGNAHOG" or "I'm a lasagna hog".

   For the next two problems, use the following symmetric cipher table:

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

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

3. Encrypt the following plaintext message: "A MAN A PLAN A CANAL PANAMA"

   Solution: O YOS O EIOS O MOSOI EOSOYO

4. Decrypt the following ciphertext message: "YOROYDYOROY"

   Solution: MADAMIMADAM or "Madam, I'm Adam"

5. What can you tell about the message in the previous problem without actually deciphering it? What does this tell you about the strength of a monoalphabetic cipher?

6. Encrypt the plaintext message "NEVER ODD OR EVEN", using a Vigenère cipher with key word "potato".

   Solution: POTATO becomes 15, 14, 19, 0, 19, 14 so we have

Plaintext	N	E	V	E	R	O	D	D	O	R	E	V	E	N
Plaintext	13	4	21	4	17	14	3	3	14	17	4	21	4	13
Keystream	15	14	19	0	19	14	15	14	19	0	19	14	15	14
Ciphertext	2	18	14	4	10	2	18	17	7	17	23	9	19	1
Ciphertext	C	S	O	E	K	C	S	R	H	R	X	J	T	B

So the ciphertext is "CSOEK CSRHR XJTB".

7. Decrypt the ciphertext "ODESL UKWGK SXMSK GEPP", which was encrypted with Vigenère cipher using the key word "octopus".

   Solution: "OCTOPUS" becomes 14, 2, 19, 14, 15, 20, 18. So we have

Ciphertext	O	D	E	S	L	U	K	W	G	K	S	X	M	S	K	G	E	P	P
Ciphertext	14	3	4	18	11	20	10	22	6	10	18	23	12	18	10	6	4	15	15
Keystream	14	2	19	14	15	20	18	14	2	19	14	15	20	18	14	2	19	14	15
Plaintext	0	1	11	4	22	0	18	8	4	17	4	8	18	0	22	4	11	1	0
Plaintext	A	B	L	E	W	A	S	I	E	R	E	I	S	A	W	E	L	B	A

   This gives "ABLEW ASIER EISAW ELBA" or "Able was I, ere I saw Elba".

8. Encrypt the plaintext message "RATS LIVE ON NO EVIL STAR", using an Autokey cipher with the key word "vital"

   Solution: VITAL is 21, 8, 19, 0, 11, so we have

Plaintext	R	A	T	S	L	I	V	E	O	N	N	O	E	V	I	L	S	T	A	R
Plaintext	17	0	19	18	11	8	21	4	14	13	13	14	4	21	8	11	18	19	0	17
Keystream	21	8	19	0	11	17	0	19	18	11	8	21	4	14	13	13	14	4	21	8
Ciphertext	12	8	12	18	22	25	21	23	6	24	21	9	8	9	21	24	6	23	21	25
Ciphertext	M	I	M	S	W	Z	V	X	G	Y	V	J	I	J	V	Y	G	X	V	Z

   So the ciphertext is "MIMS WZVX GYVJ IJVY GXVZ".

9. Decrypt the ciphertext "UBTW SEFH TTHF", which was encrypted with an Autokey cipher using the key word "cipher".

   Solution:

   "CIPHER" becomes 2, 8, 15, 7, 4, 17. So we have

Ciphertext	U	B	T	W	S	E	F	H	T	T	H	F
Ciphertext	20	1	19	22	18	4	5	7	19	19	7	5
Keystream	2	8	15	7	4	17	18	19	4	15	14	13
Plaintext	18	19	4	15	14	13	13	14	15	4	19	18
Plaintext	S	T	E	P	O	N	N	O	P	E	T	S

   Thus we get "STEP ONNO PETS" or "step on no pets."