Math 400 Fall 2018
Cryptology HW 1 Solutions
Due Thursday, September 6

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?

   Solution: The message is clearly a palindrome even before we do any decryption.

   There are many security-related things you could say about this. To my mind, the clearest insight is that you know a lot about the message even *without* decrypting it. This makes it easier to decrypt, but also means sometimes you don't have to bother.

6. Decrypt the following message, which was encrypted with a monoalphabetic substitution cipher:

   `KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ BXRME MNKNG BURIX KJRXR SBUER`
   `ISATB UIBNN RTBUM NBIGK EBIGR OCUBR GLUBN JBGRL SJGLN GJBOR ISLRS BAFFO AZBUN`

Letter	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
Frequency	16	32	5	-	7	8	22	-	16	11	13	10	8	20	12	1	1	28	7	3	14	1	2	10	-	6

Letter	B	R	G	N	A	I	U	K	O	J	L	X	M	F	S	E	Z	C	T	W	P	V	Q
Frequency	32	28	22	20	16	16	14	13	12	11	10	10	8	8	7	7	6	5	3	2	1	1	1

Bigram	NG	RI	BU	BR
Frequency	7	7	6	5

`RFAUS AGGBI NGLXM IAZRX RMNVL GEANG CJRUE KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI NJAWB OBNNO ATBZJ KOBRC JKIRR NGBUE BRINK XKBAF QBROA LNMRG MALUF BBG`

Solution:

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	o	e	c	-	m	f	t	-	n	h	i	u	y	s	l	k	j	a	g	v	r	b	p	d	-	w

I was, I think, well educated for the standard of my day. My sister and I had a German governess. A very sentimental creature. She taught us the language of flowers - a forgotten study nowadays, but most charming. A yellow tulip, for instance, means 'Hopeless Love,' while a China aster means 'I Die of Jealousy at Your Feet.'

From "The Tuesday Night Club" by Agatha Christie