CODES SUMMARY SHEET (Thanks to Dr. Carla Schultes)

Note: For the simple shift and the affine shift, encode each letter of the alphabet before you try to decipher the given messages. Write the code below the alphabet, then the letters on the bottom line are the letters in the code and the letters on the top line are the letters which belong in the deciphered message.

SIMPLE SHIFT: If x is the number corresponding to a letter, that letter is encoded by the letter corresponding to $(x+d)\ mod 26$. For example, if $d=6$, the letter B is encoded by H since here $x=1$ and $(1+6)mod26\equiv 7$ and the letter Y is encoded by E since here $x=24$ and $(24+6)mod26\equiv 30mod26\equiv 4$. Another way of looking at this is that the alphabet is shifted d letters to the left with the alphabet wrapping around on the end.

AFFINE SHIFT: In general, an affine shift follows the form $(ax+b)mod26$, where b is any integer and a and 26 have no common factors. For example, consider the affine shift given by $(3x+2)\ mod26$. C is encrypted by I since here $x=2$ and $(3\cdot 2+2)mod26\equiv 8$; K is encrypted by G since here $x=10$ and $(3\cdot 10+2)mod26\equiv 32mod26\equiv 6$; and W is encrypted by Q since here $x=22$ and $(3\cdot 22+2)mod26\equiv 68mod26\equiv 16$. There is an easier way to do this, however, if you notice a pattern forming in the way letters are assigned to other letters.

SHIFTING BY A WORD: Here you do not want to decipher the alphabet first. Instead, work only with the message given to you. To decipher an encrypted message in this assignment, write "EUCLID" repeatedly under that message, then subtract *mod*26. These numbers give you the number which correspond to the letters in the message. For example, suppose the coded message is JITAZDGNKNM. Writing "EUCLID" repeatedly under the message gives

J	I	T	A	Z	D	G	N	K	N	M
E	U	C	L	I	D	E	U	C	L	I

The numerical equivalents of these letters and their differences are

9	8	19	0	25	3	6	13	10	13	12
4	20	2	11	8	3	4	20	2	11	8
5	-12	17	-11	17	0	2	-7	8	2	4

*mod*26 these differences become

5	14	17	15	17	0	2	19	8	2	4
F	O	R	P	R	A	C	T	I	C	E

Thus the decoded message is "FOR PRACTICE." Notice that any "word" could be used for the shifting and that the process of encryption uses addition rather than subtraction.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

In-Class Group Exercise

EXAMPLES OF SOME ENCRYPTED MESSAGES

A. Decipher the following encrypted messages. Show your work.

1. SGXENGJGROZZRKRGSH, if the code is given by a simple shift with d=6.

2. AHERJOOIOQCEQXAHOCEEPSQ, if the code is given by the affine shift $3x+2 \mod 26$.

3. EHFPDHVSYSMUINJLBPELAHMQX, if the message was shifted by "EUCLID"

4. HXOJCMFQCEEKBOHSUS, if the code is one of the ones in parts 1, 2 or 3.

B. (Challenge: you may need to continue this as homework) The following quotation was encrypted using an affine shift. It is from the book *The Study of Mathematics* and the author's name is at the end of this cryptogram. He was a mathematician and philosopher whose paradox can be found on page 184 of your text.. In the film *The Mathematical Mystery Tour*, which we haven't seen yet, he is mentioned in conjunction with another mathematician/philosopher with whom he collaborated on a major work. Who is this author's collaborator and what is the title of their most famous joint work? The answer is encrypted below (in the same code as the quote).

HBEYDHBEFPX, QFRYEAN SFDZDW, CVXXDXXDX OVE VOAN EQLEY, ILE XLCQDHD IDBLENB IDBLEN PVAW BOW BLXEDQD, AFTD EYBE VK XPLACELQD, ZFEYVLE BCCDBA EV BON CBQE VK VLQ ZDBTDQ OBELQD, ZFEYVLE EYD RVQRDVLX EQBCCFORX VK CBFOEFOR VQ HLXFP, NDE XLIAFHDAN CLQD, BOW PBCBIAD VK B XEDQO CDQKDPEFVO XLPY BX VOAN EYD RQDBEDXE BQE PBO XYVZ. --IDQEQBOW QLXXDAA

collaborator: BAKQDW OVQEY ZYFEDYDBW major work: CQFOPFCFB HBEYDHBEFPB

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

C. Encrypt some messages of your own. Identify the type of encryption and the numbers or word used. On separate pieces of paper write each message with the coding technique so that another group can decode it.

1. Code a message using a simple shift. **Simple shift, d =** __ Message:_____

2. Code a message using an affine shift. **Affine shift , a=___; b=___** Message:_____

3. Code a message using a different affine shift. **a=___; b=___** Message:_____

4. Code a message shifting by a word. **word=**_____ Message:_____