EE 418 Midterm 1
University of Washington, Seattle
Fall 2004

Name: SOLUTIONS

SID#:

1. Read the questions carefully before solving them.

2. Attempt all questions.

3. You may **not use** any electronic device for calculations.

4. You are allowed to use text book, classnotes, homework problems and solutions. It is a good idea to solve problems in the order of increasing difficulty.

5. You might find the following useful:

Table 1: A correspondence between alphabetic characters and numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

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

$ax \equiv b \mod n$ has a unique solution only if gcd(a,n)=1.

$a \equiv b \mod n$ can be simplified as $\frac{a}{m} \equiv \frac{b}{m} \mod \frac{n}{m}$ where m is a divisor of a, b, n.

Good Luck and Enjoy!

Problem 1:

1. Homer Simpson wants to impress the community by proposing *mod* 27 instead of *mod* 26 for Affine Cipher. Lisa however says *mod* 29 would be better. Can you as the moderator decide whether there is any difference in the claims, and whether father's claim is better than daughter's or vice versa? Justify your decision. (Hint: how many keys are possible?) **10 points.**

   Key space of Affine cipher is partly determined by the number of values key a can take. We know that a^{-1} has to exist for decryption. With *mod* 27 **there are only 18 invertible elements** $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22\ \ , 23, 25, 26\}$**. However** 29 **being a prime,** *mod* 29 **will have 28 invertible elements! i.e.** $\{1, 2, ..., 28\}$**. Hence as usual Lisa is smarter than Homer.**

2. Inspired by the response of the community, Homer decides to go one step further and propose a modification of the Affine Cipher by including two letters (used by Homer often): " " (blank)=26, "?"=27. So there are 28 letters, hence *mod* 28 (i.e. letters $A - Z$, " ", "?"). Homer then broadcasts a ciphertext. Lisa wants to decrypt the ciphertext and hence does a frequency analysis which reveals that most common letter in the ciphertext is "B" and second most common is "T". Lisa also knows that most common letters in english text written with the 28 possible letters are " " (blank) and then "E". Can you show that Lisa is indeed successful in finding the key $K = (a, b)$ used by Homer for obtaining the ciphertext. **15 points**

   We can write:

$$1 = (26a + b) \mod 28, \tag{1}$$
$$19 = (4a + b) \mod 28. \tag{2}$$

   Solving eq (1)-(2) we get:

$$\begin{aligned} -18 &= 22a \mod 28, \\ \text{i.e. } 10 &= 22a \mod 28, \\ \text{i.e. } 5 &= 11a \mod 14. \end{aligned}$$

   i.e. $a = 3$**, and hence** $b = 7$ **from eq (2).**

Problem 2:
An ecstatic Homer decides to join a local security agency, and is asked the following two questions in the interview.

1. If attacking the Hill cipher, what plaintext would you use to *most* efficiently find the 4 × 4 key, K. Can you help Homer or is his dream of a crypto job doomed?! Show how the plaintext you are using would work efficiently in finding the key. **15 points**

   Let us denote the key matrix $K = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 \\ k_5 & k_6 & k_7 & k_8 \\ k_9 & k_{10} & k_{11} & k_{12} \\ k_{13} & k_{14} & k_{15} & k_{16} \end{pmatrix}$

   If the plaintext is *baaaabaaaabaaaab* **then we get** $\underline{x} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

   This is the identity matrix I and hence the ciphertext, $\underline{y} = \underline{x}K = IK = K$. Hence we can obtain the key K as the ciphertext.

2. Given that a plaintext *solved* was encrypted to ciphertext *GEZXDS* using a Hill cipher with a 2 × 2 matrix as the key, K, find K. (Hint: Homer fails this question since he is impatient, and tries only once. End Result: Homer's dream is doomed!) **20 points**

   ***solved*=18 14 11 21 4 3; *GEZXDS*=6 4 25 23 3 18. We know that $\underline{y} = \underline{x}K$. Hence $K = \underline{x}^{-1}\underline{y}$.**

   Finding $\underline{x}^{-1}$:
   We know $\underline{x}^{-1} = |\underline{x}|^{-1} adjoint(\underline{x})$.
   Taking $\underline{x} = \begin{pmatrix} 18 & 14 \\ 11 & 21 \end{pmatrix}$
   we get $|\underline{x}|^{-1} = 16^{-1}$ which does not exist in Z_{26}.

   Next try taking $\underline{x} = \begin{pmatrix} 18 & 14 \\ 4 & 3 \end{pmatrix}$
   with which we get $|\underline{x}|^{-1} = 24^{-1}$ which also does not exist in Z_{26}.
   So try $\underline{x} = \begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix}$
   with which we get $|\underline{x}|^{-1} = 1^{-1} = 1 \mod 26$. Therefore, $\underline{x}^{-1} = \begin{pmatrix} 3 & -21 \\ -4 & 11 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix}$.
   Hence the key $K = \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} = \begin{pmatrix} 90 & 159 \\ 583 & 704 \end{pmatrix} \mod 26$
   $= \begin{pmatrix} 12 & 3 \\ 11 & 2 \end{pmatrix} \mod 26$.

Problem 3:
Disappointed and agitated Homer tries to break into one of the agency's secret rooms. He discovers a system capable of generating ciphertexts using three different ciphers: *Shift, Affine*, and *Vigenère Cipher.* Homer takes a plaintext containing just one letter repeated a few hundered times. He makes the system encrypt the plaintext using the three ciphers (hence he now has three separate encryptions of the same plaintext). He then calls Bart and asks him to find the keys of the three ciphers. Bart is also given additional information such as the key vector length of the Vigenère cipher being $m = 10$. Can Bart accomplish the task (finding individual keys of the three ciphers)? You do not need to find the key, but simply justify your answer. **15 points=5+5+5** (*End result*: irrespective of the performance of Bart, it turns out that Homer actually broke into a recycle room with ancient machines used only during Grampa's time!)

With *Shift cipher* the key K used to encrypt plaintext is the same. Hence if the plaintext contains the same letter, say a, then the cipher essentially is the key K (repeated the few hundered times the letter is repeated).

With *Vigenère cipher* also it is possible to find K. We know that the key vector length is $m = 10$ and that the plaintext contains the same letter repeated a few hundred times. So by choosing a as the letter we get the repeating sequence of keys $\{K_1, K_2, ..., K_{10}, K_1, K_2, ...\}$ as the ciphertext.

However with *Affine cipher* we need at least two equations to solve for the key $K = (a, b)$. If the same letter is repeated in the plaintext then there will be only one equation available. Hence Bart will not be able to solve for the Affine cipher case, and Grampa can be proud that at least one of the encryptions of his time was not broken. NSA of course will not bother about it!

Problem 4:
In the meantime, the local security agency puts out a couple of questions for you to answer. They are as follows.

1. If a third-order (degree 3) LFSR sequence starts as 001110, find the LFSR expression. Note that you will have to first solve for the coefficients. Also find the next *four* elements of the sequence. **15 points**

   A third order LFSR is given as:

   $$z_{i+3} = \sum_{j=0}^{2} c_j z_{i+j} \mod 2, \tag{3}$$

   where $c_j \in \{0, 1\}$ **are the coefficients. From the given sequence, we have** $z_0 = 0, z_1 = 0, z_2 = 1, z_3 = 1, z_4 = 1, z_5 = 0$**. Hence we can write:**

   $$\begin{array}{lllll} z_3 = c_0 z_0 + c_1 z_1 + c_2 z_2 & \Rightarrow & 1 = c_2. & & \\ z_4 = c_0 z_1 + c_1 z_2 + c_2 z_3 & \Rightarrow & 1 = c_1 + c_2 & \Rightarrow & c_1 = 0. \\ z_5 = c_0 z_2 + c_1 z_3 + c_2 z_4 & \Rightarrow & 1 = c_0 + c_2 & \Rightarrow & c_0 = 1. \end{array}$$

   Therefore we can write the third order LFSR in equation 3 for the given sequence as: $z_{i+3} = z_i + z_{i+2} \mod 2$.

   The four elements are 001110$\underline{1001}$.

2. Given the sequence 0110101111000100110101111... which has period of 15, and we know that it is generated by a LFSR of degree 4. Can you express the coefficients (c_0, c_1, c_2, c_3) in matrix form (you *do not* have to solve for the coefficients). **10 points**

   The expression is:

   $$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$