HW 2 CMSC 456. DUE Sep 17
SOLUTIONS
NOTE- THE HW IS THREE PAGES LONG

1. (10 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers and on English. What is your name? Write it clearly. What is the day and time of the first midterm?

2. (20 points) (READ ON YOUR OWN about the Playfair Cipher from Wikipedia) Alice and Bob are going to use the *Playfair Cipher.* They are going to use keyword *Jeremy.* The Wikipedia article lists several possible conventions, but we will use the following: They will never use Z so they leave out Z from their encoding block. If a message has an odd number of letter then tack on a x at the end to make it even. When we need an uncommon letter for the case of two letter that are the same, we use x. Finally, fill in the rest of the alphabet in the table row by row going from left to right.

    (a) (10 points) Write down the 5×5 encoding block

    (b) (10 points) Use this table to encode *Muffin*

SOLUTION TO PROBLEM TWO

a) Note that Jeremy becomes jermy for our purposes.

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

b) Muffin! We remove capitals and punctuation and break into blocks of TWO

mu ff in

mu:

j	E	r	M	y
a	b	c	d	f
g	h	i	k	l
n	o	p	q	s
t	U	v	W	x

m,u are in diff rows and columns.

The rule is that we output the letter on the same ROW as m (the first letter) and then the letter on the same ROW as the second letter u, which is EW.

ff:

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

They are in the same column so we go to the letter below, so LY

in:

j	e	r	m	y
a	b	c	d	f
g	h	I	k	l
N	o	p	q	s
t	u	v	w	x

GP

FINAL ANSWER: EWMYGP

GO TO NEXT PAGE

3. (30 points) PROGRAMMING ASSIGNMENT.

   (a) (10 points) Write a program that does the following:

   Input: A text T of English. The first thing you do is convert the letters to numbers, $a \leftarrow 0$, $b \leftarrow 1$, etc. (and run it on a sample text. Program and output should be included in submission).

   Output:

      i. An array $A[0], \ldots, A[25]$ such that $A[i]$ is how many times i appeared in T.

      ii. An array $B[0], \ldots, B[25]$ such that $B[i]$ is the fraction of the time i appeared in T. Express as reals, not fractions. For example, we want 0.425, not 17/40. (So $B[i] = A[i]/(\sum_{i=0}^{25} A[i])$).

   (b) (10 points) Write a program that does the following. (and run it on a sample text. Program and output should be included in submission).

   Input: An array B of length 26 of reals that adds to 1 (it might be approx 1) and a number s, $0 \le s \le 25$.

   Output: Take B and circular shift it by s for form C. For example if $s = 1$ then the array C is $B[25]B[0]B[1] \cdots B[24]$. Do NOT output C. Output $\sum_{i=0}^{25} B[i] * C[i]$.

   (c) (10 points) Write a program that does the following (and run it on a sample text. Program and output should be included in submission).

   Input: A long test T.

   Output: A 26-long table of DOT-PRODUCT-ING the Freq vector from T (which you got in the first program) with circular shifts $0, 1, 2, \ldots, 25$ of itself. Output alongside the dot products the amount that it was shifted by.

   Note: We expect to find that shifting by 0 we get 0.065 or so and shifting by anything else we get 0.038 or so. If you do not get this then recheck your work but it may still be correct if your text T is unusual in some way.

GOTO NEXT PAGE

4. (20 points) In class we described the *Randomized Shift Cipher*. Describe the *Randomized Affine Cipher* and give a small example of its use (Analogous to the slides with title **How to Fix without a Long Key**, and the following slide titled **Example**. Your example should involve encoding ABAB. (Note that it should NOT map to anything of the form XYXY.)

SOLUTION TO PROBLEM FOUR

Let

$$S = \{(a, b) \mid 0 \le a, b \le 25, a \text{ is rel prime to } 26\}$$

The key is a function from S to S. To send message $(m_1, \ldots, m_L)$ (each m_i a character) Alice does the following:

(a) Pick random $r_1, \ldots, r_L \in S$.

(b) For $1 \le i \le L$ let compute $f(r_i) = (a_i, b_i)$.

(c) Send $(r_1, a_1m_1 + b_1), \ldots, (r_L, a_Lm_L + b_L)$.

To decode $(r_1, c_1), \ldots, (r_L, c_L)$ Bob does the following.

(a) For $1 \le i \le L$ compute $f(r_i) = (a_i, b_i)$.

(b) For each a_i find a_i^{-1}. It exists since a_i is rel prime to 26.

(c) Decode as $(a_1^{-1}c_1 + b_1, \ldots, a_L^{-1}c_L + b_L)$

Example:

The key is $f(a, b) = (b + 1, a + 2)$ (all of the math is mod 26). Clearly f is a bijection.

We want to code ABAB which is 0101.

Need four ordered pairs.

Pick random (2,5), maps to (6,4), so 0 maps to $6 * 0 + 4 = 4$ which is e

Pick random (3,6), maps to (7,5), so 1 maps to $7 * 1 + 5 = 12$ which is m

Pick random (10,2), maps to (3,12), so 0 maps to $3 * 0 + 12 = 12$ which is m

Pick random (15,7),maps to (8,17), so 1 maps to $8 * 1 + 17 = 25$ which is z

So Alice sends emmz.

5. (10 points) Alice and Bob are going to use the 1-time pad. They will meet and generate randomly a 999,999,999-bit key. The first message Alice wants to send to Bob is 110011. What is the probability that Alice sends 000000? How about 110011? How about 111000?

   SOLUTION TO PROBLEM FIVE

   The prob that the first message is 110011 is the prob that the key is a particular 6-bit string. Since the key is uniformly random, that prob is $\frac{1}{2^6}$. Same for all of the 6-bit strings given above.

6. (10 points) (Please do by hand – the numbers do not get that big.)

   (a) Which numbers in $\{1, 2, 3, \ldots, 14\}$ have an inverse mod 15?

   (b) For all such numbers, give the inverse.

   SOLUTION TO PROBLEM SIX

   a) The numbers are 1,2,4,7,8,11,13,14.

   b) I also tell you my thought process. One thing- we are always on the lookout for 16, 31, 46 which are all 1 mod 15.

   1 has inverse 1

   2 has inverse 8 since $2 \times 8 = 16 \equiv 1 \pmod{15}$.

   4 has inverse 4 since $4 \times 4 = 16 \equiv= \pmod{15}1$

   7 has inverse – AH, this one looks hard since none of 16,31,46 is a multiple of 7. note that $16 \equiv 2 \pmod 7$, $31 \equiv 3 \pmod 7$, $46 \equiv 4 \pmod 7$, so we need to add $3 \times 15 = 45$ to get 46+45=91. AH $7 = 91 \equiv 1$, so the inverse if 7 is 13.

   8 has inverse 2

   11 AH- noting that 2,4,7,8,13 can't work, and since $14 \equiv -1 \pmod{15}$ will be its own inverse, the only number left for 11 is … 11. $11 \times 11 \equiv 121 \equiv 1$, OH, so 11 has inverse 11.

   14 has inverse 14.