ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 16 Introduction to Communication Systems

Solutions to Homework 8 November 6, 2008

Problem 1. (a) Since the text is in the English language, the first encoded symbol, D, corresponds to either A or I. Also we know that in the English language the frequency of the letter E is maximum. Thus we might associate the symbol H in the encoded string to the letter E, since it occurs maximum number of times. With this the encoding scheme rotates each letter by 3 positions. This would imply that the symbol D in the encoded string is mapped to the letter A. With this, the plaintext is "A MATHEMATICIAN IS A DEVICE FOR TURNING COFFEE BEANS INTO THEOREMS"

(b) We apply similar kind of logic as above. We try to assign maximum frequecy symbol to the letter E and then use the knowledge of the English language to see if the assignment makes sense. For the second example if we map symbol R (which is the most frequent symbol in the encoded string) to the letter E, then we get that the third word in the encoded string, QRW, maps to the word DEJ which means nothing in the English language. Thus we can proceed to assign R to the next frequent symbol T which also results in something non-sensical in the English language. The correct assignment in this case is R → O which gives us the plaintext, "GOD DOES NOT PLAY DICE".

Problem 2. (a) Since the plaintext letter "i" is mapped to two different symbols, the cipher is polyalphabetic.

(b) Assuming it was a Vignere cipher the key used was ROUNDBALL. Use the table on page 117 of the notes to find the key.

Problem 3. The plaintext is "BARACK OBAMA YES WE CAN". Since the length of the key is 6 letters, we divide the symbols of the encoded string into the 6 groups RAWB, BOEN, KYAE, CACD, ABSA, AMEC. We then write them down as a column of letters below each letter of the key in alphabetical order: the first group RAWB is written below the letter A of the key; BOEN is written below C and so on. We then read off row-wise to find the plaintext.

C	*H*	*A*	*N*	*G*	*E*
B	*A*	*R*	*A*	*C*	*K*
O	*B*	*A*	*M*	*A*	*Y*
E	*S*	*W*	*E*	*C*	*A*
N	*A*	*B*	*C*	*D*	*E*

PROBLEM 4. (a) Let $d_1 = \gcd(a, b)$ and let $d_2 = \gcd(a, b + ca)$ for some $c \in \mathbb{Z}$. Clearly $d_2 \geq d_1$ because d_1 divides both a, b thus it also divides $a, b+ca$. Assume that $d_2 > d_1$. Clearly we have

$$\begin{aligned} a &= d_1k_1 \\ b &= d_1m_1 \\ a &= d_2k_2 \\ b + ca &= d_2m_2 \end{aligned}$$

for some integers k_1, k_2, m_1, m_2. From the last equation we see that

$$\frac{b}{d_2} + \frac{ca}{d_2} = m_2$$

Also the third equation tells us that $\frac{ca}{d_2}$ is an integer. Thus $m_2 - \frac{ca}{d_2}$ is also an integer which implies that $\frac{b}{d_2}$ is an integer. Thus d_2 divides a, b. But $d_2 > d_1$ contradicts the fact that d_1 is the gcd of a, b. Thus $d_2 = d_1$.

(b) From the first part we have

$$\gcd(a, 1) = \gcd(a - a, 1) = \gcd(0, 1) = 1$$

(c) Let $d_1 = \gcd(ma, mb)$ and $d = \gcd(a, b)$. Note that we only need to consider $m \geq 2$. We first show that d_1 is a multiple of m. Clearly we have

$$\begin{aligned} ma &= d_1k_1 \\ mb &= d_1n_1 \\ a &= dk_2 \\ b &= dn_2 \end{aligned}$$

for some integers k_1, n_1, k_2, n_2. Suppose $d_1 = ml + r$ for some l and $0 < r < m$. Then we have that

$$a = (l + \frac{r}{m})k_1$$

from the first equation. Since m does not divide r, it must divide k_1. Similarly m must divide n_1. Thus we have

$$\begin{aligned} ma &= d_1mk_1' \\ mb &= d_1mn_1' \end{aligned}$$

for some integers k_1', n_1'. Which implies that

$$\begin{aligned} a &= d_1k_1' \\ b &= d_1n_1' \end{aligned}$$

which implies that d_1 must be equal to d, since $d = \gcd(a, b)$ which is a contradiction, since md clearly divides both ma, mb thus $d_1 \geq md > d$ (since $m \geq 2$). This implies that r must be zero which means that $d_1 = ml$. As a result we have

$$\begin{aligned} ma &= mlk_1 \\ mb &= mln_1 \end{aligned}$$

Clearly $l \geq d$ and we cannot have $l > d$ as this would contradict the fact that $d = \gcd(a, b)$. Thus $l = d$.

(d) Since p is a prime and a is not a multiple of p, the only common factor between them is 1 and hence the gcd is 1.

PROBLEM 5. 1. Using Euclid's algorithm we see that the gcd is 18.

2. Using extended Euclid's algorithm we see that $72 \cdot (-4) + 306 \cdot (1) = 18$. Thus $\alpha = -4, \beta = 1$.