Handout 13 Introduction to Communication Systems
Homework 7 November 5, 2009

PROBLEM 1. Break the following ciphertexts which have been encrypted using a monoalphabetic substitution which rotates the letters of the alphabet k positions.

(a) UWTUJWYD NX F SZNXFSHJ.

(b) YGCMPGUU QH CVKVWFG DGEQOGU YGCMPGUU QH EJCTCEVGT

The first sentence is a famous quote of the mathematician Paul Erdos and the second sentence is a famous quote of Albert Einstein. Figure out what they had to say.

PROBLEM 2. The plaintext "school" is encrypted as "KKNBOW".

(a) Was the cipher a monoalphabetic or polyalphabetic cipher (Vignere cipher) ?

(b) Which key was used ?

PROBLEM 3. Decrypt the ciphertext "EIUEEBERINTSFNEAVEAVTEOEHAEHOTGTEEBEGANOWPSWRHOHACCATWTHFOIEOTIC" obtained by transposition with the key CUP OF TEA.

PROBLEM 4. (a) Prove that $\gcd(a,b)$=$\gcd(a,b+ca)$ for any integer c.

(b) Prove that $\gcd(a,b) = \gcd(a,b) = \gcd(5a+2b, b+2a)$.

(c) Prove that $\gcd(ma,mb)$=m·$\gcd(a,b)$ where m is a non-negative integer.

(d) Prove that $\gcd(a,p) = 1$ or p with p a prime number.

PROBLEM 5. 1. Find the gcd(144,60)

2. Find two integers α, β such that $\gcd(144,60) = 60\alpha + 144\beta$.