

# ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

**Handout 15**  
Homework 8

Introduction to Communication Systems  
November 6, 2008

---

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

- (a) D PDWKHPDWLFLDQ LV D GHYLFH IRU WXUQLQJ FRIIHH EHDQV LQWR WKHRUHPV
- (b) JRG GRHV QRW SODB GLFH

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 "thisisasample" is encrypted as "KVCFLTADLDDFR".

- (a) Was the cipher a monoalphabetic or polyalphabetic cipher (Vignere cipher) ?
- (b) Which key was used ?

PROBLEM 3. Decrypt the ciphertext "RAWBBOENKYAECACDABSAAMEC" obtained by transposition with the key CHANGE.

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

- (b) Prove that  $\gcd(a, 1) = 1$ .
- (c) Prove that  $\gcd(ma, mb) = m \cdot \gcd(a, b)$  where  $m$  is a non-negative integer.
- (d) Prove that  $\gcd(a, p) = 1$  with  $a \neq 0$  and  $a$  is not a multiple of  $p$  and  $p$  prime.

PROBLEM 5. 1. Find the  $\gcd(72, 306)$

- 2. Find two integers  $\alpha, \beta$  such that  $\gcd(72, 306) = 72\alpha + 306\beta$ .