T-79.4501 Cryptography and Data Security 2006 / Homework 1

1. What kind of threats the GSM security system is able to combat? What kind of threats it cannot combat?

2. The ciphertext

   FOXSFONSFSMS

   was generated using the *Shift cipher*. Plaintext is Latin. Find the key.

3. When the PT-109 American patrol boat, under the command of Lieutenant J. F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

   KX JE YU RE BE ZW EH EW RY TU HE YF SK RE HE GO YF

   IW TT TU OL KS YC AJ PO BO TE IZ ON TX BY BW TG ON

   EY CU ZW RG DS ON SX BO UY WR HE BA AH YU SE DQ

   Decrypt the first line. The key used was *royal new zealand navy*. Note that some transmission errors may have occurred.

4. The ciphertext

   VKMHG QFVMO IJOII OHNSN IZXSS CSZEA WWEXU

   LIOZB AGEKQ UHRDH IKHWE OBNSQ RVIES LISYK

   BIOVF IEWEO BQXIE UUIXK EKTUH NSZIB SWJIZ

   BSKFK YWSXS EIDSQ INTBD RKOZD QELUM AAAEV

   MIDMD GKJXR UKTUH TSBGI EQRVF XBAYG UBTCS

   XTBDR SLYKW AFHMM TYCKU JHBWV TUHRQ XYHWM

   IJBXS LSXUB BAYDI OFLPO XBULU OZAHE JOBDT

   ATOUT GLPKO FHNSO KBHMW XKTWX SX

   was generated using the *Vigenere cipher*. Use Kasiski's method to determine the keylength (period).

5. The encryption matrix (key)

$$\begin{pmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{pmatrix}$$

   of a 3×3 *Hill cipher*, where the unknown $k_i \in \{0, 1, \ldots, 25\}$, can be solved given a sufficient number (at least three) known plaintext-ciphertext pairs. Show how the computations can be simplified with a chosen plaintext attack using three well selected plaintexts.

6. Let N be a large integer. Let A and B be two sets of k numbers each formed by selecting numbers from the set $\{1, 2, .., N\}$ with equal probability. Give an estimate to k such that the probability that the sets A and B are not disjoint is about $\frac{1}{2}$.