T-79.4501 Cryptography and Data Security Autumn 2006 / Homework 1

1. Decrypt the following *Atbash* ciphertext:

   `RM GSV DLIWH LU IZNYZN RHIZVO YVORVEVW RM GSV GLIZS ZMW RM NLHSV MLG YVXZFHV LU GSV DLMWVIH GSZG GLLP KOZXV YFG YVXZFHV GSVB SVZIW GSV ELRXV LU SZHSVN HKVZPRMT`

2. The ciphertext

   `NS KFHY HQJTUFYWF FSI HFJXFW HTZQI STY RFWWD. FX WTRFS QFB XYTTI YMJ NSXYNYZYNTS TK RFWWNFLJ BFX TSQD WJHTLSNEJI GJYBJJS YBT WTRFS HNYNEJSX FSI FX HQJTUFYWF BFX VZJJS TK JLDUY XMJ BFX STY F WTRFS HNYNEJS.`

   was generated using the *Shift cipher*. Find the key.

3. Here you find the truth about the Playfair cipher. The keyword is `government`.

   `MQ AF GW EC AF GA BT RV IT BE GM QP HE HT SB SZ BA AB DI OH MV GM RV PF QA DK BQ ZS HN KD FS QA BZ AF RA BE GM PI BS GA IL DC GA BF PB DI BE QO LZ QA BA PB GM AH FN YN PW QW HO RF QR FM QA QP HE HT SB DC QF RG`

4. The ciphertext

   `VVHQW VVRHM USGJG THKIH TSSEJ CHLSF CBGVW CRLRY QTFSV GAHWK CUHWA UGLQH NSLRL JSHBL TSPIS PRDXL JSVEE GHLQW KASSK UWEPW QTWVS PGOEL KCQYF NSVWL JSNIQ KGNRG YBWLW GOVIO KHKAZ KQKXZ GYHCE CMEIU JOQKW FWVEF QHKIJ RCLRL KBIEN QFRJL JSDHG RHLSF QTWLA UQRHW DMWLG USGIK KFLRY VCWVS PGPML KASSJ VOQXE GGVEY GGZML JCXXL JSVPA IVWIK VRDRY GFRJL JSLVE GGVEY GGEIA PUUIS FPBTG NWWMU CZRVT WGLRW UGUMN CZVIL E`

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

5. Consider 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*. It is known that 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. Which of the symmetric cryptographic primitives block cipher, stream cipher, MAC function or hash function would suit best to be used as the following algorithms:

   (a) A3 algorithm in GSM, which takes takes two inputs: a secret 128-bit subscriber key K_i and 128-bit $RAND$ and produces the 32-bit response value as output;

   (b) A8 algorithm in GSM, which takes two inputs: a secret 128-bit subscriber key Ki and 128-bit $RAND$ and produces a secret 64-bit encryption key Kc as output?

7. Compute the inverse of a four-bit integer $7 = \texttt{0111} = x^2 + x + 1$ in two different arithmetic systems.

   (a) Compute the inverse of 7 modulo 16.

   (b) Compute the inverse of $x^2 + x + 1$ in Galois field GF(2^4) modulo polynomial $x^4 + x + 1$.