T-79.4501 Cryptography and Data Security
EXAM
Tuesday, December 16, 2008

1. (6 pts) 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).

2. Here is one period of a binary sequence

   $$0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0.$$

   The autocorrelation function $C(k)$ of this sequence takes values

   $$C(0) = 1, C(1) = C(2) = -1/15.$$

   (a) (3 pts) Compute the rest of the values of the autocorrelation function.

   (b) (3 pts) Does this sequence satisfy Colomb's randomness postulates?

3. (a) (3 pts) Describe the operation of Triple-DES. Explain why in Triple-DES encryption the second operation is decryption with DES, while the first and third operations are encryptions.

   (b) (3 pts) Describe the Meet-in-the-Middle attack on double encryption.

4. Consider polynomial arithmetic with polynomial x^3+x+1 on the set of three-bit integers.

   (a) (3 pts) Determine the discrete logarithm of $6 = \texttt{110}$ to the base $2 = \texttt{010}$.

   (b) (3 pts) Compute the inverse of $6 = \texttt{110}$.

5. (6 pts) Describe how the RSA keys are generated. What is the public key and what is the private key?

Exam Calculator Policy: It is allowed to use any ordinary, non- programmable calculator.