T-79.4501 Cryptography and Data Security
EXAM
Tuesday, October 28, 2008
SOLUTIONS

1. (6 pts) The ciphertext contains several strings with repetitions as indicated below:

   `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`

   The longest are

   `EGGVEYGG` repetition interval 40

   `WVSPG` repetition interval 205

   `LJSV` repetition interval 120

   By Kasiski's method one can conclude that the period of the key is at most 5.

2.

   (a) (3 pts) The values of the autocorrelation function are:

   $$\begin{aligned}
   C(0) &= C(15) = 1 \\
   C(1) &= C(14) = -1/15 \\
   C(2) &= C(13) = -1/15 \\
   C(3) &= C(12) = -1/3 \\
   C(4) &= C(11) = 1/5 \\
   C(5) &= C(10) = -1/3 \\
   C(6) &= C(9) = -1/15 \\
   C(7) &= C(8) = 1/5
   \end{aligned}$$

   (b) (3 pts) Based on the results in a) the sequence does not satisfy the third postulate R3 of Colomb (see Lecture 6, page 6). Also the second postulate R2 is not satisfied. The sequence has 8 runs (considered cyclically): `0 0 0`, `1`, `0`, `1 1 1`, `0 0`, `1 1 1`, `0` and `1`. At least 1/2 of them should be of length 1, which is true. At least 1/4 of them should be of length 2, which is not the case. And the number of runs of length 3, which should be about 1 in 8 runs is 3, which is too large.

3. (a) (3 pts) See Lecture 5, page 3.

   (b) (3 pts) See Lecture 5, pages 4-5.

4. (a) (3 pts) We search for the discrete logarithm:

   $$\begin{aligned}
   \texttt{010}^1 &= x^1 = x \\
   \texttt{010}^2 &= x^2 = x^2 \\
   \texttt{010}^3 &= x^3 = x + 1 \\
   \texttt{010}^4 &= x^4 = x(x+1) = x^2 + x = \texttt{110}
   \end{aligned}$$

   Hence the requested discrete logarithm is 4. Note: the discrete logarithm is an integer, not a bit string.

(b) (3 pts) You can use the Extended Euclidean algorithm. Another, faster way is to use the knowledge of the discrete logarithm and the fact that the order of the cyclic group formed by three-bit strings is 7, and compute

$$\texttt{110}^{-1} = (x^4)^{-1} = x^{-4 \bmod 7} = x^3 = x + 1 = \texttt{011}.$$

5. (6 pts) See Lecture 8 page 3.