T-79.4501 Cryptography and Data Security
Exam 6.3.2006

1. (6 pts) The ciphertext

   ```
   AYXHK XRGZE RIRCL ONESU RCKFE KRFXS MNSMK MSCMS KVTNE NNIWN SHGWN KZEXP
   ELXHO WOCRD USRYX EVWOG ONUAL KHGKS FUREU XHKVC APTAV EYLOA PDYLA XTETS
   UXEBO PIZCT UWCXY TORIF IMUVE YXEGH IRCTU EPVVE IMAZI MUVER SVORG RCOAV
   OCR
   ```

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

2. (a) (3 pts) What is triple encryption? What is its advantage compared to double encryption?

   (b) (3 pts) Why the middle operation of the 3DES encryption is decryption rather than encryption?

3. (6 pts) Describe the principle of the Polynomial MAC.

4. (6 pts) Alice is using a toy version of the DSA signature scheme with a prime modulus $p = 43$ and generator $g = 21$ of order $q = 7$. By accident, Alice generates signatures for two different messages with the same per-message random number k. The hashes of the two signed messages are 2 and 3, and the signatures are (2, 1) and (2, 6), respectively. Determine Alice's private key.

5. (6 pts) Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using IDEA encryption as E_K and with a counter of length 64 bits. The second box contains a true random number generator. The boxes look exactly the same, and the task is to determine which one is the true RNG just by examining the output of the generators. After both generators have produced about 2^{32} numbers, one has about 50% chance of being able to distinguish the generators. Explain why.

Remember to fill out the course feedback form at the course home page.