T-79.4501 Cryptography and Data Security
EXAM
Wednesday, September 2, 2009

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. Alice and Bob use CBC encryption. The plaintext is a sequence of blocks $P_1, P_2, \ldots, P_t$ and the corresponding ciphertext blocks sent by Alice to Bob are $C_1, C_2, \ldots, C_t$. Bob receives ciphertext blocks $C'_1, C'_2, \ldots, C'_t$, where exactly one ciphertext block C'_j has an error, where $1 \leq j < t$. Then $C'_i = C_i$ for all $i = 1, 2, \ldots, t$, $i \neq j$, and $C'_j \neq C_j$.

   a) (3 pts) Show that after decryption by Bob exactly two plaintext blocks are erroneous. What are the indices of the erroneous plaintext blocks?

   b) (3 pts) How the erroneous plaintext blocks differ from the original?

3. (6 pts) RSA can also be defined for a modulus n which is a product of three different primes. Similarly as in the usual case of RSA, the encryption exponent e and the decryption exponent d must satisfy

   $$ed \equiv 1 \pmod{\phi(n)}$$

   For $n = 1001 = 7 \cdot 11 \cdot 13$ and $e = 7$, compute d.

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) Explain the Man-in-the-Middle Attack against the basic (unauthenticated) Diffie-Hellman key exchange protocol.

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