T-79.159 Cryptography and Data Security
2005 / EXAM
Monday, 15 August 2005

1. (6 pts) The following ciphertext has been generated using the Vigenère cipher. Use Kasiski's method to determine the period.

   ```
   VKMHG QFVMO IJOII OHNSN IZXSS CSZEA WWEXU
   LIOZB AGEKQ UHRDH IKHWE OBNSQ RVIES LISYK
   BIOVF IEWEO BQXIE UUIXK EKTUH NSZIB SWJIZ
   BSKFK YWSXS EIDSQ INTBD RKOZD QELUM AAAEV
   MIDMD GKJXR UKTUH TSBGI EQRVF XBAYG UBTCS
   XTBDR SLYKW AFHMM TYCKU JHBWV TUHRQ XYHWM
   IJBXS LSXUB BAYDI OFLPO XBULU OZAHE JOBDT
   ATOUT GLPKO FHNSO KBHMW XKTWX SX
   ```

2. (a) (2 pts) Give an example of a cipher that achieves perfect secrecy.
   (b) (2 pts) Can ciphertext-only attack be used to find the key and/or the plaintext in a cryptosystem with perfect secrecy?
   (c) (2 pts) Can known-plaintext attack be used to find the key in a cryptosystem with perfect secrecy?

3. (6 pts) DESX was proposed by R. Rivest to protect DES against exhaustive key search. DESX uses one 64-bit secret key W to perform pre- and postwhitening of data and a 56-bit DES key K, and operates as follows:

   $$C = W \oplus E_K(P \oplus W)$$

   Show that a similar cipher construction

   $$C = E_K(P \oplus W)$$

   but without postwhitening, is insecure and can be broken using an attack of complexity 2^{56}.

4. (6 pts) Describe the principle of the Polynomial MAC.

5. (6 pts) Alice and Bob use Diffie-Hellman in the cyclic group of order 18 generated by $g = 2$ in modulo 19 arithmetic. Alices secret exponent $a = 7$ and Bob's secret exponent $b = 5$. Compute the Diffie-Hellman key K.