T-79.4501 Cryptography and Data Security
EXAM
May 12, 2006

1. (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

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

   but without prewhitening, is insecure and can be broken using a known plaintext attack of complexity $2^{56}$.

2. (6 pts) $2006 = 2 \cdot 17 \cdot 59$. Compute $\phi(2006)$.

3. (6 pts) Consider the polynomial arithmetic of four-bit numbers using the polynomial $x^4+x+1$. Then, all non-zero numbers form a cyclic group of order 15. Alice and Bob use Diffie-Hellman in this cyclic group with the generator element $g = 3 = \texttt{0011}$. Alice's secret exponent $a = 7$ and Bob's secret exponent $b = 4$. Compute the Diffie-Hellman key $K$.

4. Counter Mode PRNG is also called as Cyclic Encryption PRNG.
   (a) (2 pts) Explain how Counter Mode PRNG using IDEA encryption algorithm works. What size of a counter you would use?
   (b) (2 pts) Given one or more output blocks of a Counter Mode PRNG can you say something about other blocks generated by the same PRNG without knowledge of the secret key?
   (c) (2 pts) For what such a PRNG can be used in a practical security system?

5. (a) (3 pts) In PGP, which options the user has available to verify that a given public key belongs to a certain user?
   (b) (3 pts) In PGP data encryption, how does the receiver get the decryption key?