T-79.4501 Cryptography and Data Security
EXAM
Tuesday, December 15, 2009

1. Below is given one period of length $N = 15$ of a binary sequence:

   $$0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1.$$

   Autocorrelation function $C(k)$ of this sequence takes on following values: $C(0) = 1$, as usual, and $C(1) = C(2) = C(6) = -1/15$. Since $C(k) = C(N-k)$ we also have $C(14) = C(13) = C(9) = -1/15$.

   (a) (3 pts) Compute the rest of the values of the autocorrelation function for this sequence.

   (b) (3 pts) Does this sequence satisfy Colomb's randomness postulates?

2. 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:

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

   Originally two different keys were used for pre- and postwhitening, but Kilian and Rogaway showed (Crypto '96) that the same key can be used for both. Show that a similar construction

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

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

3. Consider polynomial arithmetic in the set of 3-bit integers with the polynomial $x^3 + x^2 + 1$.

   (a) (3 pts) Compute the discrete logarithm of $6 = \texttt{110}$ to the base $2 = \texttt{010}$.

   (b) (3 pts) Compute the inverse of $6 = \texttt{110}$.

4. (6 pts) Describe in detail the different steps in the generation of a key pair for the RSA public key encryption system.

5. (6 pts) Alice's data security system offers two different options for producing 64-bit pseudorandom numbers:

   - Option 1: Counter Mode PRNG using the IDEA encryption with a 64-bit counter.
   - Option 2: Counter Mode PRNG using the AES encryption with a 128-bit counter. The generator will output only the 64 least significant bits from the 128-bit output of the AES.

   Alice has selected one of these options. Eve is observing the numbers generated by Alice's system and may eventually get a proof that Option 2 was selected. After observing about 2^{32} numbers, the probability that Eve has obtained a proof is about $1/2$. Explain what is this proof and why Eve is likely to get it.

Exam Calculator Policy. It is allowed to use a function calculator, however not any programmable calculator.