T-79.159 Cryptography and Data Security
2005 / Homework 6
Tue 26.4 and Fri 29.4

1. Alice is using a toy version of the DSS signature scheme with a prime modulus $p = 47$ and generator $g = 2$ of order $q = 23$. By accident, Alice generates signatures for two different messages with the same per-messages random number k. The two hashes of the signed messages are 2 and 3 and the signatures are (4, 21) and (4, 19), respectively. Compute Alice's private key.

2. Determine the modulus m, multiplier a and increment c of a linear congruential generator given four consecutive numbers as $x_2 = 16$, $x_3 = 13$, $x_4 = 7$, $x_5 = 14$. Determine also the initial value x_0.

3. In a linear congruential generator $m = 21$, $a = 3$ and $c = 5$. A generated number $x_i = 14$ is observed. Determine x_{i-1}. Is it unique?

4. Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using Triple-DES encryption as E_K and with a counter of period 2^{64}. The second box contains a true random number generator. The boxes look exactly the same, and our 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, we have about 50% chance that we can distinguish the generators. Please, explain.

5. Let us investigate the Key Distribution Protocol depicted on slide 14 of Lecture 10.

   (a) After which message B knows that it shares the same key with A?

   (b) After which message A knows that it shares the same key with B?