T-79.4501 Cryptography and Data Security
2006 / Homework 6
Mon 27.2 and Wed 1.3

1. 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.

2. 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?

3. Counter Mode PRNG is also known as Cyclic Encryption PRNG.

   (a) Explain how Counter Mode PRNG using IDEA encryption algorithm works. What size of a counter you would use?

   (b) 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) For what such a PRNG can be used in a practical security system? How would you handle the secret key needed by the PRNG?

4. Let us investigate the Key Distribution Protocol depicted on page 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?

5. (a) In PGP, which options the user has available to authenticate a public key, that is, to verify that a given public key belongs to a certain user?

   (b) In PGP data encryption, how does the receiver get the decryption key?

6. In January 9, 2006, the Secure Shell (SSH) protocol developed by a former HUT student Tatu Ylönen reached proposed standard status in the IETF and was published as RFC 4250-4254, see `http://www.ssh.com/company/newsroom/article/700/`. The initial SSH protocol, today known as SSH-1, was soon abandonded due to its vulnerability to man-in-the-middle attacks. The proposed standard is based on an improved (but incompatible) version SSH-2. The Secure Shell Authentication Protocol is specified in RFC 4252. Describe the man-in-the-middle threat in Secure Shell and investigate which authentication options it offers.