T-110.4206 Information security technology
Examination 2013-01-02
Lecturer: Tuomas Aura
No electronic equipment or reference material allowed in the examination.

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. **Security terminology**

   Explain the meaning of the following terminology (max 20 words each):
   a) Chinese wall policy
   b) Bell-LaPadula *-property
   c) Covert channel
   d) Group-based access control
   e) NX bit
   f) Birthday attack

2. **User authentication**

   The market-leading Piggy Bank provides its customers with one-time password lists printed on paper. To log into the online bank on a secure (https) web server, a customer needs to enter (1) the online customer number and (2) the next unused one-time password. The online customer number is a 20-digit long random-looking number, which different from the user's account number and only used for the online login. Each one-time password is a four-digit number (e.g. 1:4823, 2:5349, 3:3463, 4:9913...).

   The bank is very concerned about security and wants to know if it should increase the length of the one-time passwords from four to six digits. Analyze the effect of the proposed change on the security of the system.

3. **SSL**

   Explain the principle of the RSA-based authenticated key exchange in SSL and TLS.

   (Note: You don't get any points for just listing the SSL/TLS protocol messages, but sketching the protocol may help you to write the answer.)

Please turn the paper for problems 4–6.