SECURITY ENGINEERING   FINAL EXAM   1.6.2005, 8–12

Each question is worth 5 points. The number of points for each subquestion is given in brackets (Xp means X points). Use of a **dictionary** and a **calculator** is allowed.

GOOD LUCK!

1. Give definitions or short explanations (in 2–3 sentences) for the following notions (1p for each):

   (a) Equal error rate (EER) in biometric systems;

   (b) Side-channel attack;

   (c) Tamper resistance;

   (d) Steganography;

   (e) Double-entry bookkeeping.

2. How *salted hashes* are used for storing passwords? **Draw** two schemes:

   • Storing a password (2p);

   • Checking a password (2p).

   Why hashes of passwords are stored, not passwords in cleartext (1p)?

3. In fault attacks on tamper resistant devices, what are the *methods* for fault injection (2p)? What *types* of faults may be injected (3p)?

4. How much information may be hidden in an image of size 1000x1000 pixels using the following techniques (2p):

   (a) Replacing the LSB of each pixel;

   (b) Replacing 3 least significant bits of each color component of each pixel;

   (c) The Patchwork algorithm;

   (d) Simple watermarking of JPEG images?

   Compare robustness of these schemes, clarify your answer (1p). Explain how *collusion attacks* would work in these schemes (2p).

5. What is the most powerful and most general attack on software copy protection (1p)? How is it performed, what tools are used for it (1p)? List the mechanisms that can be used to prevent it and explain how they work (2p). What mechanisms of software copy protection are essentialy useless against this attack (1p)?