Wrocław University of Technology, WPPT 18.1.08

CRYPTOGRAPHY AND SECURITY, 2007 Assignments, list # 7

1. Is it possible to run Shamir no key protocol after replacing prime number p with an RSA number?
2. Try to redesign Diffie-Hellman protocol for establishing session key so that man-in-the-middle attack does not work anymore.
3. One of the ideas to prevent a man-in-the-middle attack is the interlock protocol in which during a single round each side sends only a half of a ciphertext and then awaits a half of a ciphertext from the other side.
   Propose details of the protocol and show that it is really immune against man-in-the-middle attack.
4. Consider a simplified Kerberos in which no nounces are used. Find attacks possible in this case.
5. Design a secret sharing scheme in a group of 5 men and 5 women. The secret should be recovered by each coalition of x men and y women such that $x + 2y > 6$.
6. Let H be a hash function used to derive one-time passwords according to Lamport's method. Assume that a method for finding collisions has been found for H. Does it influence security of the one-time passwords?
7. Is the following protocol a zero-knowledge proof of knowledge of RSA key d:
   1. Alice sends a challenge x,
   2. Bob creates an RSA ciphertext c of x using key d,
   3. Alice decrypts c and checks if the result is x.
8. Transform Schnorr's authentication protocol into a signature protocol.
9. Consider a good symmetric encryption scheme E on 160-bit blocks. Define

   $$f(x, y) := E_y(x)\ xor\ x$$

   Is f a good candidate for a hash function?
10. Consider the method of hashing long messages defined by the following formula:

    $$H_i = f(H_{i-1}, x_i)$$

    where f is a good has function on blocks of a fixed size. Show that for appropriate padding this function is conflict-free, if f is conflict-free.
11. Use Floyd method to design an attack on hashing functions which does not require any noticeable memory for storing the results.

/-/ Mirosław Kutyłowski