Wrocław University of Technology, WPPT 16.11.11

CRYPTOGRAPHY AND SECURITY, 2011 Assignments, list # 5

1. Why Rabin-Miller test provides correct results in the sense that for **each** tested composite number n probability of answering “prime” is lower than one (so it does not fail like Fermat test).
2. Assume that there is a test $\mathcal{A}$ which for a given RSA ciphertext c created for an RSA number n says if the plaintext of c is smaller than $n/2$. Construct an attack which recovers the plaintext of a given ciphertext c. The attack may use $\mathcal{A}$ as a subprocedure.
3. Compare complexity of generating a pair of RSA keys of length 1024 bits and of 2048 bits.
4. One of ID-based signatures is based on a bilinear mapping $e : G_1 \times G_1 \to G_2$ in the following way:
   - A trusted authority TA has a master secret t and a public key Q_{TA} where $Q_{TA} = tP$ for a generator P.
   - A user A gets from TA a secret $S(A) = tH(A)$, where H is a hash function mapping into G_1.
   - In order to sign a message m user A chooses $P_1 \in G_1$ at random, as well as an integer k and computes:
     - $r = e(P_1, P)^k$,
     - $v = h(m, r)$, for a hash function h,
     - $U = vS(a) + kP_1$.

     Finally (U, v) is a signature for m.

   Find a verification test for such signatures.
5. Show that if there is a bilinear mapping $e : G_1 \times G_1 \to G_2$, then Decisional Diffie-Hellman problem is not hard in G_1.
6. Is it possible to run Shamir no key protocol after replacing prime number p with an RSA number?
7. Recall the game used to define Decisional Diffie-Hellman Assumption. In a similar way define security of a commitment scheme.
8. 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.
9. Formalize the property of secret sharing (n, k) saying that “less than k users cannot derive any information about the secret”.
10. 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 $x + 2y > 6$.

/-/ Mirosław Kutyłowski