MAT-52606 Mathematical Cryptology Exam 23.5.2008

Please note! This is a closed-book exam. Calculators are allowed.

1. Describe briefly the cryptosystems **a)** AFFINE, **b)** HILL, and **c)** VIGENÈRE, how they work and how they can be broken.

2. The AES cryptosystem, its usage and structure in general terms.

3. Algorithm A *breaks* a public-key cryptosystem *partially,* if

- receiving as inputs a public key k_1 and a cryptotext $c = e_{k_1}(w)$ encrypted by it, A either decrypts c and returns the corresponding plaintext w or gives up,
- for each public key k_1, A decrypts at least $100\,\theta$ % of all cryptotexts encrypted by k_1 (here θ is a known positive number which does not depend on the public key), and
- A works in deterministic polynomial time.

Show that an algorithm A partially breaking the RSA cryptosystem can be transformed to a polynomial-time Las Vegas type stochastic algorithm for breaking the system, i.e., decrypting an arbitrary given cryptotext. (As usual, for the RSA public key $k_1 = (n, a)$, only plaintexts w satisfying $\gcd(w, n) = 1$ are allowed.)

(Thus, there does not appear to be any algorithms even partially breaking the RSA system. A similar observation is valid for the ELGAMAL system, too.)

4. **a)** Construct the multiplicative group $\mathbb{Z}_7^*$, i.e. give the group multiplication table and inverses.

b) The group $\mathbb{Z}_7^*$ is cyclic. Find all generators of the group (i.e. primitive roots modulo 7). For each generator g find then the corresponding index table, i.e. the discrete logarithms $\log_g x$ for all $x \in \mathbb{Z}_7^*$.

5. Quantum key-exchange and how it differs e.g. from the Diffie–Hellman key-exchange.

Suomeksi ⟶⟶⟶