COMPUTER SCIENCE TRIPOS Part II – 2018 – Paper 8

12 Security II (MGK)

(*a*) Name *three* different families of algebraic groups that are commonly used in cryptographic applications of the Diffie–Hellman problem, where *any* group element (other than the neutral element) can be used as a generator. Briefly outline some of their main attributes, such as the set of elements and the group operator. [9 marks]

(*b*) You are preparing to participate in a password-cracking competition. During the competition, you will be given the 128-bit hash-function output MD5(p). You have to find p, an 8-character password, each character having been chosen uniformly at random from a known alphabet of 64 ASCII characters.

In the weeks preparing for the competition, you have access to a small cluster of GPU graphics cards that can evaluate MD5 10^9 times per second.

During the competition, you have only access to a laptop computer that can evaluate MD5 10^6 times per second.

Without any pre-computation, how long would it take to evaluate MD5 for all possible passwords p in a brute-force attack

(*i*) on the laptop? [2 marks]

(*ii*) on the GPU cluster? [2 marks]

You decide to use the GPU cluster to pre-compute a *rainbow table* for this challenge.

(*iii*) What functions other than MD5 will the GPU cluster have to evaluate as often as MD5 when building the rainbow table? [3 marks]

(*iv*) Your laptop has enough RAM for storing the rainbow table as a hash table of 2^{32} key-value pairs (x, y) with $x, y \in \{0,1\}^{128}$. If you execute MD5 2^{50} times while generating your rainbow table, how long will your laptop need (worst case) to find a password p stored in it, given its MD5 hash value MD5(p)? Assume that the runtime is entirely dominated by the MD5 evaluations. [4 marks]