KTH Computer Science and Communication

Homework II, Foundations of Cryptography 2014

Before you start:

1. The deadlines in this course are strict. This homework set is due as specified at `http://www.csc.kth.se/DD2448/krypto14/deadlines` and is April 1 at 15.00.
2. Read the detailed homework rules at `http://www.csc.kth.se/DD2448/krypto14/rules`.
3. Read about I and T-points, and how these translate into grades, in the course description at `http://www.csc.kth.se/DD2448/krypto14/handouts/course_description.pdf`.
4. Note that in problems with subproblem, the first number given is the total number of points for the problem and later there is information how this total is distributed over the subproblems.

The problems are given in no particular order. If something seems wrong, then visit `http://www.csc.kth.se/DD2448/krypto14/handouts` to see if any errata was posted. If this does not help, then email `johanh@csc.kth.se`. Don't forget to prefix your email subject with `Krypto14`. We may publish hints on the homepage as well.

Problems

1 (14T) Many cryptosystems like AES use a finite field of the type $GF(2^k)$ for some k. The situation is described in the book of Stinson for $k = 3$ and the irreducible polynomial $x^3 + x + 1$. Call this field F. Your task is to investigate what happens if we instead use the irreducible polynomial $t^3 + t^2 + 1$, getting a field K. The following calculations should be done by hand.

1a (2T) Compute the multiplication table of K.

1b (4T) Solve the system of equations

$$\begin{aligned} 1 + t^2 &= (1+t)y_1 + t^2 y_2 + y_3 \\ t &= (1+t^2)y_1 + t y_2 + (1+t)y_3 \\ 0 &= y_1 + (1+t)y_2 + (t+t^2)y_3 \end{aligned}$$

1c (4T) One usually speaks of *the* field with 8 elements and the reason is that F and K are isomorphic, i.e. that they only differ in the way they name the elements. In other words for each element $\alpha \in F$ find $f(\alpha) \in K$ in an invertible way such that it is always true that $f(\alpha_1 + \alpha_2) = f(\alpha_1) + f(\alpha_2)$ and $f(\alpha_1 \cdot \alpha_2) = f(\alpha_1) \cdot f(\alpha_2)$.

1d (4T) Find all such isomorphisms! Can you explain the number of such isomorphisms?

2 (8T) This problem is like the previous problem about isomorphisms but now of groups only preserving a single operation. Let $(Z_m, +)$ be the set of integers modulo m under addition and let $(Z_m^*, *)$ be the corresponding group under multiplication. To make the latter into a group it only contains the elements, a, such that $\gcd(a, m) = 1$ and thus $(Z_{12}^*, *)$ contains the elements $1, 5, 7, 11$ while $(Z_7^*, *)$ contains the elements $1, 2, 3, 4, 5, 6$. It is well known, and you may take this as given, that if p is a prime then $(Z_p^*, *)$ is isomorphic to $(Z_{p-1}, +)$ and if fact there are in general several isomorphisms of the two groups. Here an isomorphism is an invertible mapping f that satisfies $f(ab) = f(a) + f(b)$. Of course here ab is computed modulo p and $f(a) + f(b)$ is computed modulo $p - 1$.

2a (4T) Construct explicitly, by hand, all isomorphisms mapping $(Z_{11}^*, *)$ to $(Z_{10}, +)$. Can you determin the number of such isomorphisms for a a general p?

2b (4T) If $N = pq$ for two primes p and q, then can you find an additive group[1] that is isomorphic to $(Z_N^*, *)$?

3 (4T) This problems is about the term "semantically secure cryptosystem".

3a (3T) Find the definition of the term and explain the concept with your own words. Try to be formally correct.

3b (1T) Is standard RSA (i.e. encryption m by m^e modulo N) a semantically secure crypto system?

4 (4T) Suppose N is a RSA modulus, i.e. $N = pq$ where p and q are prime. Standard RSA-encryption is given by for $0 \leq m < N$ setting $c \equiv m^e$ modulo N. Remember that we require that $\gcd(e, (p-1)(q-1)) = 1$. As it is possible to recover m from the cryptotext this mapping is one-to-one. What happens if $\gcd(e, (p-1)(q-1)) = b > 1$. Is the mapping $f_e(m) = m^e$ modulo N still one-to-one? If not, can you describe which elements that are in the range?

5 (6T) There are many side-channel attacks on implementations of RSA. These are attacks like measuring time of decryption, power consumption, radiation emitted etc. Some were briefly mentioned in class. Find out more details about one such attack, write a summary in your own words (about one page in length, you may assume the reader knows basic definitions and the context) and do include correct academic references to the attack.

6 (4I) Implement Chinese remaindering. A detailed description is found on Kattis. `https://kth.kattis.scrool.se/problems/crt`. Make sure that your code is commented and well structured. Up to 4I points may be subtracted if this is not the case. Keep in mind that you must be able to explain your solution during the oral exam and please include a small summary of what you did and your kattis id in the solution set.

7 (6I+5T) It was claimed in class that knowledge of the decryption exponent d for RSA is sufficient to factor N. Locate a source that proves this, understand the proof and write it in your own words (5T). Implement the reduction (6I). A detailed description is found on Kattis. `https://kth.kattis.scrool.se/problems/rsafact`. Make sure that your code is commented and well structured. Up to 6I points may be subtracted if this is not the case. Keep in mind that you must be able to explain your solution during the oral exam and please include a small summary of what you did and your kattis id in the solution set.

[1] It might not be a group on the form just mentioned, but a direct sum of such groups.