Report on the workshop Topics in Cryptography Salahaddin university, Erbil, Kurdistan Irak, September 2012

Jorge Jiménez Urroz
Dept. Matemàtica Aplicada IV. Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona
e-mail: jjimenez@ma4.upc.edu

We arrive on saturday September first at 15:00 pm and there are 40 degrees of temperature waiting for us, at the airoport is also Herish Abdullah. Both planes Mohammed Eftekhary and mine were on time. Right from the beggining Herish is mentioning that Mohammad will not recognize the city, Erbil, since his last visit was in 2009 and things has changed a lot. New parks, new buildings, 5 universities have been created in the last for years, roads, etc. The workshop starts on September 2, so we just full the day by acomodation and dinner.

At 9:30 pm September 2 starts the workshop. It is good to remember that in Kurdistan Iraq, weekend is friday and Saturday and sunday is a normal labor day. However, this is the first day of school after the holidays, including Ramadan, that ended a couple of weeks ago. So the organizers are aware of it and let the workshop start 30 minutes after the schedule.

In his talks Mohammed address all the protocols that Cryptography can handle making some toy examples for some of them. His second talk is dedicated to hash functions and the definitions of P and NP problems needed for the talks of Herish Adbullah. My talk is about public key cryptography and I am able to complete only half of my program including a brief introduction RSA and its security based on factorization. The slides of all my talks can be obtained in the webpage of the workshop http://workshop.uni-sci.org/;

The participants are faculty and students of the Mathematical department of the college of sciences of Salahaddin university and four students from Dyala university and Sulaimani university. There were two participants expected to come from Iran but they could not attend in the last moment. The level of the participants is not too high which makes the lectures go slower than predicted. However the students make

question, take notes and try to follow the details of the lectures. The enviroment is appropriate. Fatima Aboud arrives at 13:00 pm and with Herish, Mohammad and myself we start a conversation about the future of the Kurdistan school of mathematics and the future of the workshops. We arrive to the conclusion that meanwhile the workshops should be continued, some kind change is also needed to attract more students. The idea is to increase their level so they can continue studies abroad thanks to scholarship already existing through the French embassy. The conclusion is to organize a one month intensive course in basic disciplines of mathematics, to be paid by University of Salahadin. As Herish was mentioning, the situation is so good nowadays, that the project should be done as soon as possible. During this week we will have a meeting with the president of the university.

The second day talks continue with public key cryptography and an introduction to elliptic curve. The participants are very interested about elliptic curves, and every detail has to be explained. So the material will not be covered. On the other hand, Herish gives a nice talk about his joint work with Mohammad. Herish is the director of the department, and his talks raises the interest of his colleagues presents at the lecture.

I have to finish my second talk before time since at 13:00pm I have and appointment with the spanish embassy through skype to present them the project of cooperation. I talk with Ramon Molina, the second in charge of the embassy, for about 20 minutes. He seems very enthusiastic about the ideas of the workshop, the intensive courses and the main goal which is the foundation of the Kurdistan school of mathematics. He shares the opinion that Kurdistan now is making big changes and politicians defend the idea of increasing the support for education. He ensures me that he will get in touch with the French embassy and politicians from Kurdistan as soon as possible. I commit myself to send him the letters of support of our project from the EMS and IMU

On Tuesday we had two talks one by Mohammad about using hash functions for data integrity and the second one of Herish explaining their joint work. I had proposed on monday a change in their proposal and they already have given me an answer. I insist in other change and again they corrected. On the other hand, at the middle of the talk a very interesting discussion in Kurdish and arabic starts among many participants and Herish. It is clear that this collaboration will have a very good impact in the mathematics department of Salahaddin university and, in the future, collaborations of this type with mathematicians from Irak and from abroad will be a very good motivation for increasing the level of mathematics in Kurdistan. At the end of the talk, we had a meeting with the president of the university. The president supports completely our initiave. In particular, we mention the need of a complete funding from the university of Salahadin for the succed of the proposal

and he agrees and push the initiave trying to make it real as soon as possible. In fact, we are again lucky and the university has just lauched the new phd program in which it fits our proposal. A document will be given to the president in a week and we will try to start the project in January 2013.

In the afternoon Herish took us to make some tourism around Erbil. It is fantastic the progress the city is doing. We visited a mall which is as if we were in Europe. It is shocking to think that 12 years ago everything was in ruins. We should take advantage of the current situation to impulse the Kurdistan school of mathematics.

Wednesday is my last day lecturing and I am really behind my program, so I decide to give an overview. The participants are very interested on elliptic curves, in principle, so I suggest after the workshop they make a small group to work on it. I offer myself to help them answering whenever possible. After that, Herish ends presenting his joint work with Mohammad. At the beggining of the class we have proposed an exam to the participants to be solved and return on thursday. The two students with the highest mark will get a T-shirt from CIMPA and the DVD Dimensions. They seem excited about the idea.

Thursday is the last day of talks. Mohammad explains Elgamal criptosystem, its elliptic curve version, and two attacks for the discrete logarithm, brute force and Babystep giant step. After his talk, we solve the exam. For each problem there is a student, or more,. willing to go to the blackboard to solve it, even that sometimes the solution is incorrect. There are two teams and then two women that tried alone each of them. We appreciate the eforts of not being part of a team and each of the women win the T-shirts. Each team wins a DVD.

After that we hace a lively discusion in Arabic about the workshop, and the project of the Kurdistan school of mathematics is also presented to the participants. They are really excited about the idea.

After the workshop is finished, we have a meeting with the scientific comitee of the department to discuss the time, and contents of the first intensive course. It will be part of the master program, for a month, and will be given in the second semester, around April. This first course will be in Analysis since it seems common interest to any master student. The idea is to change the subject in different courses. There will be a professor from the department of mathematics of Salahadin university helping in the preparation of the exercises and with the idea that in the future he will be the main profesor. There will be around 25 hours of theory and around 20 of exercises. We have another meeting with the dean, but the previous with the scientific comitee lasted longer than expected and the dean had to leave. He give us excuses but had another appointment.

Friday is free and we visited Shaqlawa. A holy place in which three religions joint together. Christians, Muslims and Zoroastrians. We have to climb a bit in a mountain to reach a cave. Shaqlawa is 45 minutes from Erbil by road and there are three police controls in between. One can see that the soldiers on each control are completely relaxed and even though there is a heavy traffic there is no jam at the control. During the trip we see the huge investment happening in Kurdistan nowadays. There is construction all along the road. Hotels, appartments, recreation areas, etc. The situation in Kurdistan Irak is completely calm. Tomorrow we leave the country.