Math/Mthe 418/818

Term Project

Due 29 November 2017

Rules: This project is to be done in teams. This means that each person of the team should be involved in every part of the project.

Suggestion: Before starting any MAPLE code, hand in a first draft of parts (a) – (d) of the project by 13 November 2017.

Background Scenario: Your team is employed by a company that wants to market an El Gamal cryptosystem. Management has decided to allow any potential client to be able to choose the key size (bit-size) of the public key (within reason). It is your task to design an El Gamal cryptosystem that is secure and has this flexibility.

Notes: 1) In the real world, you would have to guard against all known attacks. For purposes of this project, however, you are asked to guard only against the log-table attack and the Silver-Pohlig-Hellman attack.

2) If the client picks a bitsize for which no secure key can be found, then your program should pick a (larger) key size which is secure. It should inform the client of the fact that the chosen key size cannot be used and that the key size xxx was used instead.

1. (a) Describe the ElGamal cryptosystem (over \( \mathbb{F}_p \), where \( p \) is a prime) for sending secret messages and explain why it works: (i) why the receiver recovers the original message; (ii) on what the security of the cryptosystem depends.

(b) Describe the log-table attack and the SPH attack on the discrete logarithm in \( \mathbb{F}_p \). Explain under what circumstances each of these can be applied, and what are the consequences for the design of cryptosystems using the discrete logarithm method in \( \mathbb{F}_p \).

(c) Design a protocol for a key generation scheme of an ElGamal cryptosystem for message transmission in \( \mathbb{F}_p \) which actively guards against these two attacks and which works for arbitrary (large or small) bitsize. Give a step-by-step description of your design and explain how it guards against these attacks. More precisely, your protocol should construct, for a given input bitsize \( n \), a key \((p, g, y)\) which is safe against these attacks and for which \( p \) has bitsize \( \geq n \). Moreover, each call of the protocol should produce a different key.

(d) Give another method for finding \( p \) and \( g \) (as in part (c)) and discuss the expected pros and contras for each.

(e) Implement both methods in a MAPLE program, and test your methods by finding a key \((p, g, y)\) for the input bitsize \( 23 \div \log_2(10^7) \). Use Maple’s timing feature to compare the time that your two methods take to compute a list of 100 keys with input bitsize \( 66 \div \log_2(10^{20}) \). (Do not display the full lists, but only the first two and last element of each.)
(f) Pick your best design of part (d) and incorporate it in your ElGamal cryptosystem. Implement this as a sequence of three separate MAPLE programs: (i) key generation for ElGamal; (ii) encryption; (iii) decryption.

(g) Let $m = 123456789098765432101234567890123456789$. Use your program to encode and decode the message $m$ twice, using primes $p$ of bitsize 300. Time your key generation.

**Remark:** See the file “Maple instructions” on the web for basic instructions about MAPLE homework and documentation and the file “Term Project: Comments and Hints” for further instructions and clarifications.