COMP3491 Codes and Cryptography
2021-22 Summative

Maximilien Gadouleau

1 Pollard rho for elliptic curves (50 marks)

Alice and Bob have used Elliptic Curve Diffie Hellman in order to share a 56-bit DES key. Using the shared key, Alice then encrypted a short message to Bob. The resulting ciphertext, together will all the relevant information for the ECDH key exchange, are given in `ECDH.txt`. Your task is to implement Pollard Rho for Elliptic Curves, use it to determine the shared key, and decrypt the message.

Basic Pollard rho (20 marks)
Implement basic Pollard rho, which finds a collision of the form $cP + dQ = c'P + d'Q$ and returns c, d, c', and d'.

Full Discrete Logarithm solver (10 marks)
Implement full Pollard rho, based upon the basic implementation above, which goes through the list of potential logarithms if $\gcd(d' - d, n) > 1$ and returns the discrete logarithm from that list.

Decryption (20 marks)
Based on your Pollard rho implementation, determine the shared key and decrypt the ciphertext.

I will verify that your Pollard rho code works. Examples of input/output are given in `exampleInputRho.txt` and `exampleOutputBasicRho.txt` and `exampleOutputFullRho.txt`.

2 Shortest Vector Problem (50 marks)

Implement one of the four techniques to solve SVP (Lecture 12), find a short vector for the lattice whose basis is given in `latticeBasis.txt`, and write a report on your implementation.

Difficulty (15 marks)
Depending on which technique you use, you will be awarded at most the following marks:

- Enumeration (4 marks)
- Sieving by differences (8 marks)
- Sieving by averages (12 marks)
- Modified sieving by averages (15 marks)

Quality of implementation (20 marks)
You must return the shortest vector that you can find on the lattice. The student who returns the shortest vector amongst their peers will be awarded 20 marks; other students who return a valid lattice point will then be awarded partial credit. Students who return points that are not on the lattice will be awarded 0 marks. Instructions on the format of the output are given in `exampleShortVector.txt`.

Report (15 marks)
Write a short report (no longer than 3 pages, 11pt font, margin at least 2cm) describing the design choices, heuristics, and optimisations used in your implementation. Marks will be awarded for originality, clarity, and soundness.

3 Submission checklist

1. Code for Basic Pollard rho.
2. Code for Full Pollard rho.
3. Text file with decrypted plaintext for Pollard rho.
4. Code for SVP.
5. Text file with shortest vector for SVP.
6. Report for SVP.