The University of Sydney
School of Mathematics and Statistics

Assignment 2

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

Like Assignment 1, this assignment is in two parts: a "non-computer part" and a "computer part". Each part consists of two questions: in the non-computer part, which two questions you need to do depends on whether you are enrolled in the mainstream unit MATH2068 or the advanced unit MATH2988; in the computer part, all students do the same two questions. Each part will be marked out of 10 and is worth 5% of your total mark, so the assignment as a whole is worth 10% of your total mark.

Both parts of the assignment must be submitted through Turnitin on the MATH2068 Blackboard page or the MATH2988 Blackboard page, as appropriate. Note that there is a separate Turnitin submission for each part; **please make sure you submit the right file to the right Turnitin submission**. On the Blackboard page, the submission links appear in the menu on the left as "MATH2068 Assignment 2 Non-Computer Part" and "MATH2068 Assignment 2 Computer Part", or the equivalent with MATH2988. You do not need to submit the two parts at the same time, but the same deadline applies to both of them.

For the non-computer part, your submission can be either typed or a scan/photo of handwritten answers, but it must be submitted as a single file that can be viewed in Turnitin: for example, a single PDF or a Word document, but **not a Zip file**. Check that your file displays correctly in the Turnitin preview window before you submit it. **Unviewable or illegible submissions will get a mark of 0.** For the computer part, your submission will be a text file which is the record of a MAGMA session (perhaps edited), and should be given the name "asst2-[sid].txt" where "[sid]" is your student ID.

As always with Turnitin, a submission is not complete until you see the Digital Receipt, including the submission ID number and time. You should either print this Digital Receipt or email it to yourself so that you have a copy, for each of the two submissions; in the (unlikely) event of database error, this Digital Receipt is the only acceptable proof of the time of your submissions. It is your responsibility to leave enough time before the assignment deadline to complete both Turnitin submissions: **if you forget to do a Turnitin submission before the deadline, or fail to complete the submission, you will get 0 for that part of the assignment even if you can prove that you did it before the deadline**. If you discover a problem with a file you have submitted, you can submit a new version before the deadline (which will simply replace your previous submission).

Except for students who have registered with Disability Services or who apply successfully for Special Consideration or Special Arrangements (see the Information Sheet), the due date for this Assignment is **Thursday 26 October, 2017**, before **11:59pm**.

Non-computer part: Write or type complete answers to the two questions appropriate to the level of unit you are enrolled in, showing all working.

1. **This question is for students enrolled in the mainstream unit MATH2068 only. Do not answer this if you are in the advanced unit MATH2988.**

   (a) Suppose that you are an Elgamal user with public key $(107, 2, 30)$ and private key 12. Note that this is consistent, because $2^{12} \equiv 30 \pmod{107}$. If you receive the ciphertext $\langle 3, [51, 74] \rangle$, what is the decrypted message?

   (b) Find a primitive root modulo 43. Justify your answer.

2. **This question is for all students.**

   (a) Find an integer $x \in \{0, \ldots, 196\}$ which solves the equation

   $$x^{131} \equiv 12 \pmod{197}.$$

   (b) With help of primitive roots or otherwise show that for any prime $p > 3$ there exists $n \in \{2, 3, \ldots, p-2\}$ such that the polynomial equation

   $$x^n \equiv x + 1 \pmod{p}$$

   has an integer solution.

3. **This question is for students enrolled in the advanced unit MATH2988 only. Do not answer this if you are in the mainstream unit MATH2068.**

   (a) Let n be a positive integer. Show that for any factorization of $n^2 + 1$ as a product of two positive integers, $n^2 + 1 = a \cdot b$, one has $|b - a| \geq \sqrt{4n - 3}$.

   Hint. Think about the following idea: If $|a - b|$ is "small" then a and b are "close" to n.

   (b) Describe the polynomial time algorithm which, given $n \in \mathbb{Z}^+$, finds an integer m such that $|m^3 - n|$ is minimal possible.

   Note: You need to show that your algorithm always gives a correct answer and explain why it is polynomial time. You do not have to provide a rigorous computer code for it, "human" description will suffice. (However, if you are able to write MAGMA code for the algorithm, you could of course then test actual large numbers to see whether it works and whether the growth rate of the time appears to be as expected.) Also, you do not have to produce as quick algorithm as possible. Any polynomial time algorithm will suffice.

Computer part: This is to be done using MAGMA, either in the computer labs (the lab session in Week 12 has been set aside for this purpose) or on your own computer if you have successfully installed MAGMA there (see the instructions on the unit web page). If you are completing Q5 outside the computer labs, you will need to download the file asst2definitions.txt from the Resources Table on the web page.

What you need to submit is a "log file" or record of your MAGMA session; to get MAGMA to generate this automatically and give it the right name, you can make your first command `SetLogFile("asst2-[sid].txt");` where `[sid]` is replaced by your student ID. You could answer the two questions in different MAGMA sessions, but in that case you would have to concatenate the log files (e.g. using a text editor) so that you have a single text file to submit to Turnitin. In case of problems with the `SetLogFile` command, you can alternatively create the text file yourself by copying and pasting from your MAGMA session into a text editor.

As well as the MAGMA commands, you may wish to add comments such as "Question 4" or "This is my answer": you can start and end comments by typing `/*` and `*/`.

If you complete the assignment in the labs, you could (probably) do the Turnitin submission there too, but in any case please **email yourself a copy** of your log file(s).

4. In MAGMA define `p` to be the smallest prime which is greater than or equal to your student ID and is also congruent to 1 modulo 4. Ask MAGMA to choose a primitive root `b` modulo `p` with the command `b:=PrimitiveRoot(p);`. Then use appropriate MAGMA commands to find a nonnegative integer less than `p` which is a square root of -1 modulo `p`. There are two such integers; you can stop once you have found one of them, except that you should then get MAGMA to check that your answer does square to something congruent to -1 modulo `p`.

5. Load the file asst2definitions.txt. It defines an RSA public key (`n`,`e`) and a ciphertext `ct` which has been encrypted using this public key; `ct` is a sequence of residues modulo `n`, which happens to consist of just a single residue. (To avoid antagonizing Turnitin, it is best not to print `n`, `e` or `ct` in your MAGMA session. If you want to see them, look in the file asst2definitions.txt.)

Before encryption, the original message (four words in ordinary Roman letters) was encoded as a residue modulo `n` using the `NaiveEncoding` function in the file MagmaProcedures.txt. Your task is to find this original message by decrypting `ct` as in Computer Tutorial 6, for which you will first need to find the decryption exponent `d`, the inverse of `e` modulo ϕ(`n`).

The problem is that `n` has 1250 decimal digits, which is far too large to use the MAGMA commands `Factorization(n);` or `EulerPhi(n);` (don't bother trying them; MAGMA will just hang or run out of time). This RSA cryptosystem would be unbreakable, except that someone has let slip the information that the two primes of which `n` is the product are a Germain prime x and its corresponding safe prime $2x + 1$. Knowing this, you can find x as the unique positive solution of the quadratic equation $2x^2 + x - n = 0$. To apply the quadratic formula, you will need to find the square root of the discriminant `D` as an exact integer: Q4 of Computer Tutorial 8 explains how to do this.