University of London

Computing and Information Systems/Creative Computing

CO3326 Computer security

Coursework assignment 2 2018–19

IMPORTANT: all students have been allocated a unique set of data to use for this coursework assignment. You can obtain this using your Student Reference Number (SRN) from the following URL: http://foley.gold.ac.uk/cw19/api/cw2/{srn}. For example, if your SRN is 877665544, you would obtain your data from http://foley.gold.ac.uk/cw19/api/cw2/877665544. If you have difficulties obtaining your assignment data, please email us at: intcomp@gold.ac.uk

This coursework assignment is designed to help you enrich your learning experience and to encourage self-study and creativity. Chapter 9 (pages 95-103) of the subject guide, including the suggested supplementary reading, will help you in completing this assignment. You should read the coursework assignment very carefully and pay particular attention to the Submission requirements.

You are expected to submit **two** files: a **report** and a **results sheet**. The *report* counts as **60%** of your coursework assignment mark, in which you are expected to answer the questions below. The *results sheet* counts as **40%** of your mark, in which you are expected to summarise the results of your calculations in a specific format. Please use the cipher text and keys provided when answering the questions and when compiling the results sheet.

To complete the coursework assignment, it will make your life easier if you write a program. You are welcome to use any programming language.

Coursework assignment 2

This coursework assignment takes a practical example for the El Gamal public key cryptosystem. The notation is similar to the one used in your subject guide (section 9.4, pages 99 - 101). **IMPORTANT:** To answer the questions below, please use the coursework 2 assignment data that you obtained using your SRN.

Question 1 Verify whether p is an actual prime (*i.e.* not just a probable prime). Provide a brief explanation and include the method from your code, as well as the runtime.

Question 2 What is the computational complexity of your primality check? Presumably, you have a loop; how many steps does it take relative to p? Include the code where you calculate this.

Question 3 Discuss briefly how you can go about optimising the primality check, including a code snippet.

Question 4 Verify whether g is a generator for p. Provide a brief explanation and include the method from your code, as well as the runtime. **Hint:** As p is a 16-digit prime, the definition from your subject guide is not a practical way to verify whether g is a generator. You will have to research on how El Gamal is implemented in practice (for example in Open SSL) – you will find that p is a special kind of prime.

Question 5 Considering that a is Alice's private key and b is Bob's private key, compute their public keys and show how they can generate the same shared key. Include a brief explanation and the relevant code snippet.

Question 6 Decrypt the provided cipher text which has been encrypted with the shared key that you computed in Question 5. Include a brief explanation and the relevant code snippet.

Question 7 Suppose Alice and Bob want to generate a new set of keys. They decide that they should use a 17-digit prime instead. How would they go on about generating a new p and a corresponding generator g? Provide a brief explanation and include the relevant code snippet, as well as its runtime.

Question 8 Generate a new set of private and public keys for Alice and Bob, using the p and g you generated in Question 7. Encrypt your SRN with the shared key. Include a brief explanation and the relevant code snippet.

Submission requirements

REMINDER: It is important that your submitted coursework assignment is your own individual work and, for the most part, written in your own words. You must provide appropriate in-text citation for both paraphrase and quotation, with a detailed reference section at the end of your coursework. Copying, plagiarism and unaccredited and wholesale reproduction of material from books or from any online source is unacceptable, and will be penalised (see our guide on how to avoid plagiarism on the VLE).

You should upload **two** single files only. These must not be placed in a folder, zipped, *etc.*

The **report** should be submitted as a PDF document following a *strict naming scheme*: `YourName_{srn}_CO3326cw2.pdf`. For example, Steve Jobs with SRN 877665544 would submit `SteveJobs_877665544_CO3326cw2.pdf`.

The **results sheet** should be submitted as a JSON file with a *strict format* and *strict naming scheme*. This summarises the results of your calculations and will be automatically checked by an algorithm, so pay particular attention to its format. The name of the file should be `YourName_{srn}_CO3326cw2.json`; for example, Steve Jobs with SRN 877665544 would submit `SteveJobs_877665544_CO3326cw2.json`.

Example

You have obtained your coursework assignment data in the following format (this is an example for illustration):

```
{
  "srn": "877665544",
  "name": "Steve Jobs",
  "exercise1": {
    "p": "2685735182215187",
    "g": "2",
    "a": "3628281929",
    "b": "5915661551",
    "cipherText": {
      "encoded": "65462432711955",
      "base64": "O4mpDEUT"
    }
  }
}
```

For this, Steve Jobs would submit the following JSON, which reflects a correct solution:


```
{
  "srn": "877665544",
  "name": "Steve Jobs",
  "exercise1": {
    "p": "2685735182215187",
    "g": "2",
    "a": "3628281929",
    "b": "5915661551",
    "x": "1611247168640770",
    "y": "1057465508852156",
    "k": "1133299385179611",
    "cipherText": {
      "encoded": "65462432711955",
      "base64": "O4mpDEUT"
    },
    "plainText": {
      "encoded": "427071729268",
      "base64": "Y291bnQ=",
      "text": "count"
    }
  },
  "exercise2": {
    "p": "44685735181995023",
    "g": "5",
    "a": "4628273483",
    "b": "6915587579",
    "x": "3934012106049896",
    "y": "6387156331543282",
    "k": "16887845058447247",
    "cipherText": {
      "encoded": "27261997930282270",
      "base64": "YNqkhoB9Hg=="
    },
    "plainText": {
      "encoded": "877665544",
      "base64": "NFAdCA=="
    }
  }
}
```

Explanation

The *srn* and *name* fields are self-explanatory. *exercise1* is relevant for questions 1 to 6 from the report. *exercise2* contains the results of questions 7 and 8. The notation is similar to the notation used in section 9.4, pages 99 - 101, in the subject guide: p is the prime, g is the generator, a is Alice's private key, b is Bob's private key, x is Alice's public key, y is Bob's public key, k is the resulting shared secret key.

In Exercise 1 the plain text has been encoded with Base64, which has been transformed to a number. If you are using Java, there are utilities provided by Apache or Google, among others, to do these operations. Similar libraries exist in other programming languages. If you struggle with these operations or you would like to double-check your results, you can use the web API calls below. For Base64 encoding/decoding you can use the following:

- http://foley.gold.ac.uk/cw19/api/cw2/encode?text=count
- http://foley.gold.ac.uk/cw19/api/cw2/decode?base64=Y291bnQ=

For text encoding/decoding to/from numbers, you can use the following:

- http://foley.gold.ac.uk/cw19/api/cw2/toNumber?text=Y291bnQ=
- http://foley.gold.ac.uk/cw19/api/cw2/toText?number=427071729268

obviously replacing `count`, `Y291bnQ=` and `427071729268` with the text or number you want to encode/decode.

In both the *plainText* and *cipherText*, the *encoded* is a number, the *text* is an English dictionary word and the *base64* is a Base64-encoded text. As in *exercise2* you have a number to encrypt (your SRN), the *text* field is irrelevant.

Final note

You can use the example solution above as a template, which is a well-formed JSON, and replace the values with your data and calculation results. As the JSON will be evaluated by an algorithm, every quote, comma, colon, curly brace upper/lower case is crucial. Please pay attention to these. It would be a shame to lose a potential **40%** of the total marks for this coursework assignment because of a misplaced comma or a missing quote. There are online tools you can use for JSON formatting and validation (for example https://jsonformatter.curiousconcept.com), so double-check that your JSON is syntactically correct.

[END OF COURSEWORK ASSIGNMENT 2]