MANCHESTER METROPOLITAN UNIVERSITY

School of Computing, Mathematics & Digital Technology

ASSIGNMENT COVER SHEET

Unit:	Introduction to Computer Forensics and Security 6G7Z1009
Assignment set by:	Dr. Majdi Owda and Dr. Liangxiu Han
Verified by:	Dr. Soufiene Djahel
Assignment number:	1CWK50
Assignment title:	Portfolio; two components
Type: (GROUP/INDIVIDUAL)	INDIVIDUAL
Hand-in format and mechanism:	Moodle Submission
Deadline:	14th of December 2018

Learning Outcomes Assessed:

1. Critical analysis and evaluation of the digital forensic process in terms of technical and legal aspects.
2. Analyse and evaluate volatile and non-volatile data.
3. Explain, critically analyse, compare basic cryptographic algorithms and propose appropriate uses for them.
4. Explain, critically analyse a variety of security attacks, basic security protocols and propose corrections to simple defective security protocols.

It is your responsibility to ensure that your work is complete and available for assessment by the date given on Moodle. If submitting via Moodle, you are advised to check your work after upload; and that all content is accessible. Do not alter after the deadline. You should make at least one full backup copy of your work.

Penalties for late hand-in: see Regulations for Undergraduate Programmes of Study: http://www.mmu.ac.uk/academic/casqe/regulations/assessment.php. The timeliness of submissions is strictly monitored and enforced.

Exceptional Factors affecting your performance: see Regulations for Undergraduate Programmes of Study : http://www.mmu.ac.uk/academic/casqe/regulations/assessment/docs/ug-regs.pdf

Plagiarism: Plagiarism is the unacknowledged representation of another person's work, or use of their ideas, as one's own. MMU takes care to detect plagiarism, employs plagiarism detection software, and imposes severe penalties, as outlined in the Student Handbook (http://www.mmu.ac.uk/academic/casqe/regulations/docs/policies_regulations.pdf and Regulations for Undergraduate Programmes (http://www.mmu.ac.uk/academic/casqe/regulations/assessment.php). Bad referencing or submitting the wrong assignment may still be treated as plagiarism. If in doubt, seek advice from your tutor.

Assessment Criteria:	Indicated in the attached assignment specification.
Formative Feedback:	Formative Feedback will be provided on weekly basis in the lab sessions.
Summative Feedback format:	Grid provided as part of the marking scheme.
Weighting:	50%

1. Assignment Description

1.1. Part 1: Digital Forensics

Description

The assignment task is to write a report (up to a max 1,000 words excluding the references and abstract) that concludes your investigation on the following case study to submit as an expert witness statement.

Case study:

You are a digital forensics investigator working at a high tech. crime unit. You have been given a suspect evidence file to investigate, i.e. a forensic image of the suspect machine hard disk. The suspect has been accused of involvement of black-mailing. The suspect name is Bob Hunter. You will need to investigate the forensic image and record your findings and then create an expert witness report to present to the court.

Note: You will be given the forensic image “HunterXP.E01”.

The report should include the following subsections:

1) Report title and investigator name (your name).
2) Abstract
3) Introduction
4) Report Body (present and highlight your findings)
5) Conclusion
6) Personal Reflection
7) References

In terms of formatting, the report should follow font “Times New Roman, size 11 or 12” and the citations should follow the Harvard reference format.

Assignment Marking Scheme

a. Report structure, approach, references and proper critical analysis 30%
b. Report Findings 70%

1.2. Part 2 Information Security

Description

This part consists of four tasks, which examines students' theoretical and practical knowledge in relation to basic cryptographic algorithms and security protocols.

Task 1

1.1 Explain the difference between DHM (Diffie-hellman-Merkle) and RSA using diagram and mathematical formulas whenever possible. Give the reason why RSA is hard to break.

1.2 Show the working steps on calculating a shared key for a secret cipher using the DHM with parameters p=7 and g=4, and implement it in python.

Task 2

2.1 In RSA, let e=5, n=55. Can you find $d \equiv 1/e \pmod{\varphi(n)}$? Why?

2.2 Let e=13, n=55. Find $d \equiv 1/e \pmod{\varphi(n)}$ provided that d exists. If d does not exist, explain the reason of the nonexistence of d.

2.3 Given the RSA public key (3,70747) and private key (46811,70747)

- Encrypt the letter 'z' using its ASCII value.
- Decrypt the result from the subtask 2.4 above and generate the original text.
- Encrypt the word 'Hello' two characters at a time padding with a space.
- Decrypt the following three blocks 14520 66071 27623. The blocks are the encryption of a five-letter word, encrypted two characters at a time and padded with a space. Recover the word.
- Determine the maximum block size, in bits, that this modulus can encrypt and decrypt.

Task 3

Alice used a password to create a zip file secret.zip which contains only a secret.txt file. The secret.txt file contains really important information that Alice would like to access. Unfortunately, Alice forgot the password she used to create the zip file. Alice only remembers that the password is a six-digit password. Given the secret.zip file, you are asked to help Alice to recover the password with an implementation in Python.

Task 4

4.1 Critically compare, analyse and evaluate three authentication protocols including Needham-Schroeder protocol, Otway Rees, Kerberos.

4.2 Given Alice wants to communicate with Bob over an insecure network, you are required to 1) design a protocol based on a shared secret key to allow them to authenticate each other; 2) Explain the limitation of using the shared secret key in this context.

2. Staff availabilities and formative feedbacks

Staff availabilities (Office Hours) are displayed on the unit Moodle area for providing help and support students learning.

The formative feedbacks will be provided on a weekly basis during the lab sessions.

3. What to hand in

You will need to submit your report through Moodle submission inbox, which is highlighted at the top of the unit Moodle area. You will need to submit your report as one PDF file if possible. In addition please use the following naming structure for your report before uploading it to Moodle (“your lastname-firstname-studentID.pdf”).

Part 1 Marking Scheme:

The report will be assessed as follows:

Report structure, approach, references and proper critical analysis	30%
Report Findings	70%

Note: You will need to attempt all sections to get the full range of marks.

Part 2 Marking Scheme:

Your work will be assessed as follows:

Tasks	Task 1	Task 2	Task 3	Task 4
Marks	30 Marks in total including: 20 marks for subtask 1.1 and 10 marks for subtask 1.2 respectively	30 marks in total including: 10 marks for three subtasks respectively	10 marks	30 marks in total including 20 marks for subtask 4.1 and 10 marks for subtask 4.2

Note: You will need to attempt all sections to get the full range of marks.