EBU6010 Cryptography and Cyber Security

COURSEWORK (2023/24)

EBU6010 gives an overview of the principles and practice of network security, which aims to provide an insight into the technical security features that allow establishing safe communication methods over networks. In particular, it focuses on the functionality, strengths and vulnerabilities of the existing network security features and the different encryption/decryption and security protocols.

As part of the course plan, students are required to prepare a coursework in the form of a mini-project comprising a practical component (simple cryptography quizzes) and an essay on the wider scope of data security. The overall coursework counts for 20% of the final course mark.

1. Practical exercises [100 marks]

1.1 In this section of the coursework is a Public-Key procedure practice. In this you will need to demonstrate your knowledge in creating key-pairs for RSA:

[Add the last two-digits from your QM number and process the resulting plaintext/number (*m*) using the RSA algorithm]; i.e. if your last two digits are 87, then m=8+7=15.
You will not receive any marks for this section if you do not use your student ID number correctly.

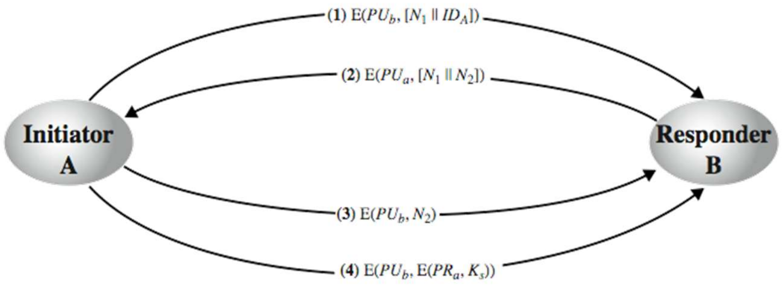
a) If person **A** needed a Private-Public key pair, and they have generated the following: ***p***=3, ***q***=11, ***e***=7; find ***d*** to form the key-pair. Is this possible? If yes, provide the answer, if not, explain why not.

b) Use the following parameters to generate a pair of private and public keys for **B**, where ***p***=11, ***q***=17, ***e***=7.

Apply the private-public key pair to:
(i) Generate the cipher *c* by encrypting *m* (from **B** to **A**).
(ii) Decrypt the generated cipher *c* (when received by **A** from **B**).
(iii) Explain the steps and calculate final ciphertext if **A** would like to send message *m* to **B** providing both authentication and confidentiality.

Your answer must provide explanation of the key generation and encryption procedure, and should also highlight the resulting value for ***c*** for each of the scenarios above.

1. 1.2 A hacker performing a man-in-the-middle attack by intercepting message (4), attempting to send the session key, K_s to B using the following message: $E(PU_b, E(PR_h, K_s))$. Will the hacker succeed? Explain your answer.


(1) E(PU_b, [N_1 || ID_A])
(2) E(PU_a, [N_1 || N_2])
Initiator A
Responder B
(3) E(PU_b, N_2)
(4) E(PU_b, E(PR_a, K_s))

2. The essay **[100 marks]**

The mini-research / essay paper should be no more than 2000 words. The essay should be aimed for the benefit of both technical engineers and anyone from the general public. Students can choose to work on any of the following topics:

- Recent advances in Secure Hash Algorithms (SHAs): a focus on standards and applications;
- Applications of block-chaining techniques for data security;
- Challenges associated with data security of IoT applications.

Background and materials for the assignment:

In order to complete your task appropriately, your report should be based on:

➢ Thorough understanding of the given task.
➢ Research into the topic area using books and other resources.
➢ Materials from lectures.

That is, it should reflect your own interpretation and comments not just repeating someone else's ideas. Technical issues, including equations and algorithms, are welcome but a purely technical report will give you a lower grade.

Coursework specifications

Here are some guidelines that should help you to present your work logically and clearly:

- You need to produce an essay for one of the given topics. The number of words should not exceed 2000 words – you may lose marks if it exceeds this limit.
- Your work should be fully referenced, and all references must be from textbooks, publications, or respectable internet sites, in IET or IEEE format. You are expected to use diagrams and/or figures where appropriate.
- Identify the main issues to consider and the lines of arguments within the selected topic, and be specific.
- Use clear and understandable English to present your work, which should follow a logical structure:
  - Introduction: What are you going to say in the essay?
  - Body of the essay: present your main points accurately and fully. Demonstrate that you understand your topic.
  - Conclusion: Put everything together, summarise your main points.
  - References: Source(s) of information.

Paper format:

The document used should follow the following formats:

Font	Times New Roman or Arial
Size	12 pt
Margins (Standard A4)	Standard margins
Page Numbers	Pages MUST be numbered
File Format	**.pdf**

The coursework is set as an assignment on QMPlus; it **must be submitted in PDF format**.

Assessment criteria

Pass: To obtain a pass you will need to complete the following:

- Appropriate structure and presentation of the paper.
- Clear and correct use of English.
- The paper should be fully researched and referenced appropriately.
- The researched topic is presented in your own words.

Distinction: To obtain a Distinction your work should

- Fulfil all the criteria for Pass with all parts correct.
- Include a thoughtful discussion on the selected topic.

Marks Distribution

The coursework marks are distributed as follows:

Aspect	Marks %	Pass %
Structure and presentation of paper	20	~8
Evaluation and explanation (possible use of examples)	40	~16
Referencing and citation, evidence of background reading	20	~8
Use of clear and correct English	20	~8
Total	**100**	**40**

Plagiarism:

Plagiarism is treated very seriously and could lead to **FAIL** marks for the coursework or the entire course!

Plagiarism includes:

- The use or presentation of the work of another person as your own work (or as part of your own work) without acknowledging the source.
- Submitting the work of someone else as your own
- Extensive copying from someone else's work in your own paper or report.

Papers will be checked for plagiarism through the *TurnitIn* platform.