School of Computing: assessment brief

Module t	ptography
Module c	MP3223
Assignment title	Coursework 2
Assignment type and description	Coursework assignment
Rationale	Learning the mathematical basis of asymmetric cryptosystems
Weighting	20% of total mark
Submission deadline	March 31st 2023 at 16:00
Submission method	Turnitin submission through Minerva
Feedback provision	Feedback provided on Minerva
Learning outcomes assessed	(i) Understand and apply in practice the fundamental principles of cryptography and information security. (ii) Analyse and evaluate the strengths and weaknesses of cryptosystems. (iii) Apply mathematical analysis to understand how asymmetric cryptosystems are constructed.
Module lead	Dr Toni Lassila

1. **Assig**

   Provid ree exercises below. Answer all three exercises.

2. **Asses**

   Exerc llowing questions on group theory.

   (a) Consider the multiplicative group $G = (\mathbb{Z}_{26}^*, \cdot)$. Show that the inverse of any element $g \in G$ can be found as $g^{-1} \equiv g^{11} \bmod 26$. **[3 marks]**

   (b) Consider the multiplicative group $G = (\mathbb{Z}_{119}^*, \cdot)$.

      i. Is G cyclic? Justify your answer. **[1 mark]**

      ii. Find the solution $x \in G$ of the equation

      $$11x \equiv 3 \bmod 119$$

      using extended Euclid's algorithm. **[4 marks]**

Exercise 2: The following exercises are on primality testing.

(a) Is $n = 721$ a (Fermat) pseudo-prime in base $a = 46$? Explain how to test a number for pseudo-primality. **[2 marks]**

(b) Use the Miller-Rabin Primality Test to test whether $n = 721$ is a strong pseudo-prime in the base $a = 46$. **[3 marks]**

(c) Is $n = 721$ prime? How can we use the Miller-Rabin test to find this out given the result of b)? **[2 marks]**

Exercise 3: Alice and Bob use the RSA cryptosystem for encrypted communications.

(a) Show that the multiplicative property holds for RSA, i.e., show that the product of two ciphertexts y_1,y_2 is equal to the encryption of the product of the two respective plaintexts x_1,x_2:

$$y_1 y_2 \bmod n = RSA_e(x_1 x_2).$$

[2 marks]

(b) B[illegible]rypted message y_1 from Alice using the RSA k[illegible]ponent n. Eve obtains y_1 by eavesdropping a[illegible] some other plaintext x into a ciphertext y u[illegible]e and the exponent n. She then sends Bob a [illegible]$= yy_1 \bmod n$. Bob doesn't suspect anything a[illegible]nd that corresponding plaintext x_2 doesn't m[illegible]iscards it. Eve is then able to obtain x_2 too. Describe a chosen-ciphertext attack against RSA in this setting that allows Eve to obtain the original plaintext x_1 from the information known to her. Which condition should x satisfy for this attack to work? [3 **marks**]

3. **General guidance and study support**

   The MS Teams group for COMP3223 Cryptography will be used for general support for this assignment. If your question would reveal parts of the answer to any problem, please send instead a private message to the module leader on MS Teams.

4. **Assessment criteria and marking process**

   Assessment marks and feedback will be available on Minerva within three weeks of the submission deadline. Late submissions are allowed, standard late penalties apply.

5. **Presentation and referencing**

   When writing mathematical formulas, use similar notation and symbols as during the lectures and tutorials. Hand-written sections for mathematical notation are acceptable but need to be clearly readable.

   You may assume theorems and other results that have been presented during lectures and tutorials as known. Any other theorems need to be cited using standard citation practice.

6. **Submission requirements**

   Submit your answers through Turnitin as one PDF document (generated either in Word or with LaTeX). You may use hand-written and scanned pages for mathematical formulas, but these need to be clearly legible and the document must contain at least some typeset text or Turnitin will reject in. All submissions will be checked for academic integrity.

7. **Acade[illegible]and plagiarism**

   Acade[illegible] engaging in good academic practice. This involve[illegible]e skills, such as keeping track of where you find id[illegible]n and referencing these accurately in your work.

   By sul[illegible]ment you are confirming that the work is a true e[illegible]n work and ideas and that you have given credit to others where their work has contributed to yours.

8. **Assessment/marking criteria grid**

   Total number of marks is 20, divided as follows:

   Exercise 1 (multiplicative groups): 8 marks
   Exercise 2 (primality testing): 7 marks
   Exercise 3 (RSA cryptosystem): 5 marks