Friday 22 May 2020, 09:00 BST
(24 hour open online assessment – Indicative duration 1.5 hours)

DEGREES OF MSc, MSci, MEng, BEng, BSc,MA and MA (Social Sciences)

Cryptography and Secure Development (M)
COMPSCI 5079

(Answer All 4Questions)

Th **arks**

1.

(a) What is the entropy of a message space and how is it used in cryptography? Explain why the concept of entropy is useful?

[2]

(b) Calculate the entropy of the following message space in which the message "Nothing Special" occurs with probability 1/2 and the messages "Rain", "Snow", "Ice" and "Gales" each occur with probability 1/8.

[4]

(c) Define the term “redundancy of a language” and give a formula to calculate it in terms of various rates of a language. How can these rates be calculated?

[2]

(d) A system authenticates users by asking them to enter an 8 character password. Estimate the entropy of this password system if the users use lower case English words as their passwords. Describe how a practical attack that exploits this low entropy could be mounted.

[7]

2.

(a) Describe with [illegible] encryption algorithm, ex [illegible] ters of the plain text are entered and letters of the resulting cip [illegible] is the encryption key entered? How is the cipher text decrypte [illegible] l plain text?

[3]

(b) Give an example of a 4 rotor machine where each rotor implements a Caesar cipher with shifts 3, 15, 7, 4. The alphabet consists of the 26 English letters plus space, comma, fullstop. Show how your machine both encrypts and decrypts?

[6]

(c) How would you use your rotor machine to avoid the mistakes that led to the ENIGMA rotor machine being broken.

[6]

3.

(a) An simple version of the RSA public key system is based on the two prime numbers 5 and 11. The encryption key is 3, calculate the decryption key. State the public and secret keys.

[6]

(b) Explain why 4 cannot be an encryption or decryption key. List all the possible encryption and decryption keys.

[4]

(c) Calculate the cipher text if the plaintext is 4. Explain why this system will not encrypt the plain text 45 properly and state 2 more plain text values that cannot be encrypted properly.

[5]

4.

(a) What is a moral hazard, also known as a perverse incentive? Give 3 examples of moral hazards with a security context.

[4]

(b) What is a security threat model and how can it constructed? How is it related to an attack surface and a security target? Give an example (not one from your course notes).

[8]

(c) Give an example of a Misuse Cases and show how can it be used in an Agile development setting.

[3]