CS4614 - Introductory Network Security

Exam number: ☐☐☐☐☐☐

This questionnaire is automatically read by a computer program. Please use a pen for filling in your answers.

Check: ☒ Respond by placing an 'X' in the box next to the chosen answer.

Uncheck to correct: ■ You can correct an answer once, as shown on the left. This cannot be undone.

IMPORTANT: All answers should be provided in the spaces provided on this paper. You must write your exam number on each page.

1 Choice Questions

Answer all of the following questions by choosing one answer per question. Each question is worth 1.5 *marks. There will be 30 such questions in the exam, for a total of* 45 *marks.*

1.1 Security attacks are classified as either passive or aggressive.

☐ True ☐ False

1.2 The family of techniques used for deciphering a message without any knowledge of the enciphering details is known as _____.

☐ blind deciphering
☐ cryptanalysis
☐ steganography
☐ transposition

1.3 _____is when each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

☐ Substitution
☐ Streaming
☐ Diffusion
☐ Permutation

1.4 The sender is the only one who needs to know an initialization vector, when used by a cipher mode of operation.

☐ True ☐ False

1.5 SHA-1 produces a hash value of _____ bits.

☐ 224
☐ 384
☐ 160
☐ 256

2 Problems

Answer all of the following questions in the spaces provided on this paper. Each question is worth 15 *marks. There will be 3 such questions in the exam, for a total of* 45 *marks.*

2.1 What requirements must a public key cryptosystem fulfil to be a secure algorithm?