The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 5 Solutions

4th April 2019

Number of Questions: 5
Time allowed: 50min
Total marks: 5

In order to score marks you need to show all working/reasoning and not just the end result.

	Student Number	*Student Name*
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	Question 2	Question 3	Question 4	Question 5	Total

1. In a running key cipher, the key is as long as the plaintext. The key is often a text from a well-known book (e.g. chapter 5, paragraph 3 of "To Kill a Mockingbird"). Is such a system equivalent to a one-time pad (achieves perfect secrecy)?

- If so, outline why it is impossible to gain any knowledge about the contents of the plaintext regardless of how much is intercepted.
- If not, state at least one difference between a running key cipher and a one-time pad, and outline a possible approach to attacking a running key cipher.

Assume, if necessary, that the attacker is able to mount a chosen plaintext attack – that is, the attacker can put a chosen new plaintext through the system and obtain the corresponding ciphertext.

Solution:
No, because the key is not random, it is possible to use frequency analysis to reduce the number of likely plaintexts and keys.
Further, the key is reused, thus by doing a chosen plaintext attack, the attacker is able compare the plaintext with the ciphertext to obtain the key.

2. Estimate the unicity distance of a monoalphabetic substitution cipher, assuming that all keys are equally likely.

Solution:
U = lg(26!)/3.2 = 27.62

3. How many different encipherments can you get with a Rotor machine with 6 rotors? (Rotor machine has 26 input pins on front and 26 output pins on back)

Solution:
Formula: 26^k, where k is number of cylinders.
For k=6: number of enciperments = 308 915 776

4. A famous example of a rotor machine is Enigma, which was used by the Germans in World War II. What were some of the factors that enabled the Allies to break Enigma?

Solution:

- Reuse of keys
- Highly structured military messages

5. The following ciphertext was produced using a Vigenere cipher with 4 alphabets:
RMLKLCFXPAGALMAXTGBYWMEYLKGLLKEXJG

The frequency analysis is displayed below. Find the plaintext and the key.

```
Graphing Frequency Counts for 4 alphabets.

Graphing alphabet 0

                      *
                      *
                      *
                  *   *       *   *   *     *
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Graphing alphabet 1

                        *
            *       *   *
*   *       *       *   *
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Graphing alphabet 2

        *   *
* *     * * *         *
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Graphing alphabet 3

                                              *
                                              * *
*                   * *                       * *
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

Solution:
Plaintext = key reuse is the enemy of perfect secrecy