**CSC 301 Lab 01: IDs, Passwords, and Authentication**

Points: **100** points.

**Format:**

* File type: Word file (.doc or docx).
* File name: LastName\_FirstName\_Lab01
  + e.g. Bond\_James\_Lab01.doc
  + Add your name also as a header as seen with assignment title.
* Font: Times New Roman.
* Font size: 10.
* Page number: at the bottom.
* Line and Paragraph Spacing: 1.0

**Rules:**

* Keep it short, keep it simple.
* No long paragraphs or essays.
* Please answer systematically using short itemized bullets.
* Simply write the question number followed by the answer.
* *You will lose points up to %10 not following the exact format rules explained above.*

1. [15 points] Can we use the legal system (Laws, regulations, Police forces, Prosecutors, etc.) to protect computer systems? Support your answer with *three* reasons.
2. [15 points] When police investigators perform DNA analysis are they doing *identification* or *authentication*? And why? Explain your answer.

1. [25 points] Describe A dictionary attack can be augmented to try orthographic substitutions, such as 2 for z and @ for a. Assume a common dictionary has 100,000 words and (to make calculations easy), all letters are lower case and the 26 letters are evenly distributed (that is, “a” occurs exactly 1/26 of the time as does “z”). How many extra substitute word possibilities are there, allowing @ for a? (That is, the attack would try the word “bay” and also “b@y”.) If there are ten such orthographic substitutions (2 for z, @ for a, 1 for I, 6 for b, $ for s, etc.), how many word possibilities would an attacker need to try?

1. [15 points] If a user is prohibited from using any of the most recent *n* passwords, why should the system still protect those passwords from viewing, just as strongly as it protects the current password? Give *three* reasons.

1. [15 points] Discuss the security impact of a biometric device that sends simply “yes” or “no” to the computer to show the user passed or failed authentication, versus one that sends a full representation of the biometric credential to be evaluated on the computer. For example, a user might insert a coded card (with his or her biometric pattern secretly encoded) into a reader and then place a finger over a print reader. The reader can then inform the computer that the user did or did not match the pattern described on the coded card.

1. [15 points] Must identities be unique? Must authentication data be unique? Explain your answer.

**- The End -**