1. Define each of the components of CIA as it pertains to computer security. \((30\text{pts})\)

Confidentiality
- Data confidentiality - assures the private or confidential information is not made public
- Privacy – individuals control what information related to them is collected

Integrity
- Data integrity – information and programs changed only in an authorized manner
- System integrity – system performs its intended function

Availability
- Systems work promptly and are not denied to users

2. Give one argument for and one argument against the statement, “Symmetric encryption is the best encryption method”. \((20\text{pts})\)

\textbf{Argument for:}

Performance

\textbf{Argument against:}

Need for a shared key.

3. What defines the strength of a hash algorithm? \((10\text{pt})\)

The length of the hash value.
4. What is the technical difference between DES and Triple-DES? Why is Triple-DES more secure? (20pt)

Triple DES is DES run 3 times. The strength of Triple-DES comes from having multiple keys, which effectively increases the key size.

5. Which is more secure, single-key encryption system or two-key encryption? Why? (20pt)

Neither. For the most part, the strength of the algorithms is based on the size of the key.