**ADELYN L. SALDIVAR**

**IT36A**

**CAESAR CIPHER**

* The Caesar cipher is a straightforward encryption technique dating back to ancient Rome, named after Julius Caesar, who reputedly employed it for military communication. In its simplest form, each letter in the plaintext is shifted a fixed number of positions up or down the alphabet. For instance, with a shift of 3, "A" becomes "D", "B" becomes "E", and so forth. The cipher operates under the principles of substitution, where each letter is replaced by another letter. Despite its simplicity, the Caesar cipher can provide a basic level of confidentiality for messages, especially in historical contexts. However, it is highly vulnerable to brute-force attacks due to its limited key space of 26 possible shifts. Therefore, it is not suitable for secure communications in modern times but remains a fundamental concept in the study of cryptography.