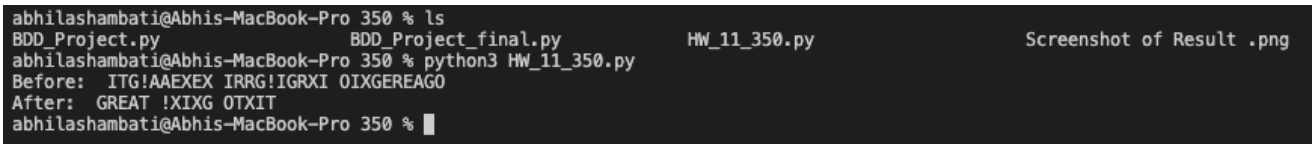
1. 

Plain Text: GREAT !XIXG OTXIT

2. To solve this issue, we modified the Huffman algorithm to operate on bits rather than bites. If the tree has already been built, the priority heap will be set up so that a node with a lower probability is assigned a greater priority. The procedure is largely the same, but we will need to convert it to account for the digits.
   Therefore, the left child will represent the modification digits (0–4), while the right child will represent the modification digits (5–9). After setting up the tree, we must walk over it and convert each node to a number code. If a node is not a leaf node, we name the edge to the left child of that node with a random number between 0 and 4, followed by the ASCII value of that symbol, starting at the root. The right node, not a leaf node, receives the same treatment. After following the procedures to encode the complete tree, we will have a digit code rather than a bit.

3. The process in which we validate a cryptographic protocol is called cryptanalysis.
   There is a variety of techniques that can be deployed to attack. One way to do this is by brute force method in which we attempt every possible phrase to crack the code. This is a resource-exhaustive method as there could be lots of possibilities.

   Modern protocols include the AES crypto protocol. It is frequently employed since it is thought to be secure and nearly impossible to decrypt. Despite the difficulty of decrypting AES, many have opted to target the algorithm's implementation rather than the cipher text itself. This is what is known as a side-channel attack, and it is a modern method for determining whether cryptographic algorithms are vulnerable.