CS4355 Cryptanalysis

Final project – question 3

Dec.7/19

Avery Briggs

3471065

In the scenario where Alice wants to have her files available on the cloud storage service, securely and efficiently, she would need to take a few preparation steps to improve the chosen model.

For her files to remain secret to attackers or eavesdroppers, she should implement some sort of encryption on her files to increase obscurity. To improve on this further, she could use an individual AES encryption on each of her files, to obtain n different keys from Fn different files. This ensures that even if one file’s key is compromised, that the whole system won’t be compromised. One further step to increase obscurity one more level, would be to then encrypt each individual file key into one larger file so she can utilise only one key on her machine for local purposes.

As for the performance of the system, that could be improved by implementing a better data structure, like a balanced binary-search tree. This search tree would work well because it would match the desired search time O(log(n)). An additional strength to the balanced binary search tree, is that it fulfills the condition of having no way to identify which file came from which set. That is because the tree won’t be distributed in a way where the directory is immediately the parent node of the subdirectories.

The above improvements could be implemented in this system, I believe without compromising or hindering the final product. Since the encryption and decryption of files using the keys is done client-side, the server is only reliant on the search time. The worst-case search time for finding an element in a BST matches our desired threshold. And the nature of balancing a BST offers confusion and obscurity of being able to concretely map out the original file hierarchy.