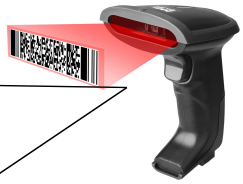
Data Security Diagram

A001234567



A#s are scanned in by students

A001234567 + Salt123

A00123456
7Salt12345

A#s are 'salted' this means that giberish not found in the dictionary is added to provide resistance to rainbow and hash table attacks. origional a# is overwritten is discarded never stored in a database.

Hash Algo

A#+salt is then entered into military grade encryption hash algorithim and turned into a Hash token. Hashing is a one way mathmatical operation where even if the algorithm is known such as SHA-256 the math is such that it is computationally unfeasable to try to reverse the algorithm. A#+salt is now discarded.

2cf24dba5fb0
a30e26e83b2
ac5b9e29e1b
161e5c1fa74
25e730e93b0
e58a9f470b1

Hash Token + UserName

Tokens are generated in <1 seccond. If there is no matching token in the database then the user is prompted enter a username. Username and token will then be placed in the encrypted database so that even if an attacker decrypts the database they will be left holding some gibberish and usernames.