Farid Rajabinia - fr2md

- **What is the string that has the MD5 hash of abc20d7bde1df257f890e152af2e3470? How did you determine this?**
  It is decoded as dictionary, I just used an online hash decoder to reverse the hash.
  https://md5hashing.net/hash/md5/abc20d7bde1df257f890e152af2e3470

- **What is password salting? Why would we use it?**
  Password salting is a way to make password hashing more secure particularly in case of rainbow table attack (a predefined list of passwords and their hashes). By adding a random number - that is called salt - into the hash function of the password, we can create a unique password for each user that can not be determined by the rainbow table attack.
  This is the formula to create the hash: Hash(password+salt).
  Now there is no way for pattern matching with the most common password hashes, the only known way to break this hash is to brute force.
  https://learncryptography.com/hash-functions/password-salting

- **What is a dictionary attack? When is it used?**
  This is another way of brute forcing all possible passwords for an account or the keys for encryption/decryption process. Social engineering can explain its success: people tend to choose familiar words or phrases (i.e. meaningful words that might be found in a dictionary as their password). Therefore, by almost brute forcing all possible words, we might be able to crack the password. I do not know how, but in Wikipedia it is said that compared to other brute force techniques, dictionary attack "a dictionary attack tries only those possibilities which are deemed most likely to succeed."
  This attack can be eliminated if the account is locked after some incorrect guesses. It can also be stopped by choosing the combination of uppercase lowercase letters and numbers and special characters.
  https://en.wikipedia.org/wiki/Dictionary_attack