Brute force, Dictionary and Rainbow discussion

A brute force attack or exhaustive attack, the attacker tries all possible passwords in an automated fashion through probing the complete key space on the algorithm, It attempts to determine a secret by trying every possible combination.

A dictionary attack means that you probe only passwords from a dictionary, which does not contain the complete key space. A brute force attack is primarily used against the encryption algorithm itself. A dictionary attack is primarily used against passwords. Encryption algorithms are seldom attacked with a dictionary attack because most times they use a random number as key. A typical dictionary for this attack would contain the most used passwords. A rainbow table is used to attack a hashed password in reverse. That means I have a table with possible hashes and look up a matching password. To prevent attacks using rainbow tables each hashed password should be differently salted as then I would need a rainbow table for every hash and every salt.