Q1

Figure A: SKC

Figure B: ASKC

Q2

1. Cipher text 1 is the encrypted message, cipher text 2 is the encrypted symmetric key
2. Cipher text 1’s encryption key is done using the secret key shared between both parties (symmetric key), cipher text 2’s encryption key is done using the receiver’s public key
3. Size of cipher text 1 is larger than cipher text 2. As the message is usually larger than the symmetric key size.

Q3

1. If the attacker hacks into the database, a salt makes the hash of the same passwords different preventing attackers from seeing which user’s password are the same and hence, hacking more accounts.
2. A salt makes the hash output random protecting against dictionary attacks where attackers try the hash of common user passwords to hack into their accounts.