1) Encryption can not be done in parallel because every block depends on the output of the perious block.

Decryption can be done in parallel because you only need the cipher text.

2) 64/8 = 8 blocks
It also affects the decryption of the cipher text block.

8+1 = 9

3) A sends a request to B. It sends the ID of A, a nonce, and a key

B sends the ID's of A and B to KDC. It also send a nonce and key for a as well as a nonce and key for B.

KDC responds with two encrypted blocks. One block is for B. It has a session key, A's ID, and and B's nonce. The other block is for A. It contains a session key, B's ID, and A's nonce.

Finaly, A's encrypted block is passed back to A

3b) The level of security is the same. The proposed scheme tries to "connect with b before interacting with KDC. This can avoid overhead if B refuses a connection.

4) Discretionary Control: control based on the identity of the requester and rules that describe what requesters can do.

Mandatory: Control based on comparing labels and security clearences.

Role Based: Based on the roles in an organization

Attribute based: Attributes or labels are given to all entities, these labels are used to decide who can access what.

Teacher is a role, so it would be role based.