1. A known plaintext attack is when the attacker knows what some of the characters or words of the plaintext are as encrypted ciphertext. A block cypher of 8 bits means that there are only 256 possible values for the 8 bit byte, so if the attacker already knows some of the plaintext and cipher text, they can easily create an algorithm to decrypt the rest and future messages that use the same secret key. One way they can do this is using brute force, in which the attacker tries all possibilities. Again, in this case, it would not be hard because there are only 256 options for each block. Another way is that the attacker could create some sort of cryptogram or table where they can map already known pairs and build off of that using probable words, common letters, patterns, etc.
2.

a) From this scheme, an eavesdropper could still discern certain patterns and make connections based off of them. If two blocks had the same encrypted data, the attacker would know that the decrypted data will be the same. Also, the attacker would know that the encrypted block of data is the exact same size as the decrypted block.

b) An attacker could change the message received by sending blocks of data of the same size with bad data. They could also swap the order of blocks or even delete them. This would all result in incorrect data being sent.

c) To prevent these kind of attacks, you could use cipher block chaining where the output of the previous of the previous block is XOR'ed with the plaintext of the current block. Also, it uses an initialization vector which is used to help with randomization. This is less prone to attacks because it hides patterns that are possible to detect when just using ECB. You could also add a signature to each message using RSA. If Alice signs her message she sends to Bob with a valid signature, Bob should be able to verify by getting the message back from the signature with the use of Alice's public key.