1. **Describe BEAST attack scenario in detail, which is the chose-plaintext attack on CBC mode in TLS 1.0.**

BEAST attack uses the vulnerability of CBC which is the Initial Vector(IV) used to encrypt the first block is fairly easily predictable.

The basic mechanism of the attack starts with a MITM(Man In The Middle) who has knowledge of the plaintext as well as the IV. Using the IV which stays the same and the plaintext the attacker first injects a random block of bytes so that the first character of the plaintext is located in the last character of the block. For instance, if the plaintext is “JayHello” in a 8-byte-block then the MITM encrypts the first block with “ILoveMeJ” such that the first letter ‘J’ is now located at the end of the block. In this way, the attack has a high chance of guessing the decrypted character. Likewise, the attacker repeats this for the remaining characters to find out the decrypted message eventually.

1. **Find the countermeasure fixed in TLS 1.1 and demonstrate why this is the case.**

The crucial precondition of the BEAST attack is the attack has successfully guessed the IV. Therefore, the approach TLS takes is to introduce an explicit IV that differs for each block. When Sending each block of the message, TLS 1.1 generates a unique IV. Due to this, the attack now has to find IV every time he/she wants to conduct a BEAST attack. However, without any knowledge of the IV, decryption is not possible, thus this solves the vulnerability of TLS 1.0.