Question 1

CBC-HMAC

Information an attacker can learn about decrypted *valid* messages:

- Message length: The padding validation is implemented in my code by string comparison. The time it takes to compare the two strings is proportional to the length of the padding. Variability in message lengths will cause variability in the padding lengths, which will cause variability in validation time.

Information an attacker can learn about decrypted *invalid* messages:

- Correctness of padding/tag: Assuming the message is invalid, it will be detected either because of the padding or because of the tag. The time it takes to receive the validation error can leak information about whether the both validations ran or just the first one (which would mean the padding was invalid).

PKCS-1.5

Information an attacker can learn about decrypted *valid* messages:

- Block type 0: Since blocks with block type 0 can be ambiguously interpreted, such blocks require additional validation which would increase processing time.
- Message length: similar to the case in CBC-HMAC.
- Private key: as we learned in the second lecture, *assuming* exponentiation is implemented using the "square and multiply" algorithm, precise timing enables an attacker to extract the full private key (or at the very least discover how many bits are '1').

Information an attacker can learn about decrypted *invalid* messages:

- Block type 0: when the padding is invalid, if the reason is ambiguity of padding then the code will terminate at a specific point, which will affect its running time.