Cipher Block Chaining Message Authentication Code (CBC-MAC)

1. **To prove the security of CBC-MAC**, we define a game between an attacker and a defender. The attacker's goal is to create a message that passes the CBC-MAC check, while the defender's goal is to detect any message that has been tampered with.
2. **Assume the attacker's ability-** We assume that the attacker has access to a CBC-MAC oracle, which can generate a MAC for any message that the attacker chooses. The attacker is also allowed to make a limited number of queries to the oracle.
3. **Analyze the MAC construction-** We analyze the construction of CBC-MAC and observe that it uses a block cipher to encrypt the message in a block-wise fashion. The MAC is then generated by taking the last encrypted block as the output.
4. **Observe the property of CBC-MAC-** We observe that CBC-MAC has the property of strong unforgeability, which means that it is computationally infeasible for an attacker to create a new message that has the same MAC as an existing message. This property holds as long as the block cipher used in the construction is a secure PRP.
5. **Construct a new message-** Assuming the attacker is able to create a new message that passes the CBC-MAC check, we can construct a new message by appending the crafted message to an existing legitimate message.
6. **Analyze the new message-** We analyze the new message and observe that it will not pass the CBC-MAC check, because the MAC of the new message will be different from the MAC of the original legitimate message. This is because the MAC is computed

using the last encrypted block of the message, which will be different for the new message.

7. **Build a new message-** Given the inability to create a new message that passes the CBC-MAC check, the attacker is unable to forge a new message that has the same MAC as an existing message.
8. **Conclusion-** We conclude that **CBC-MAC is a secure MAC** construction as long as the block cipher used in its construction is a secure PRP. The security of CBC-MAC is based on the property of strong unforgeability, which makes it computationally infeasible for an attacker to create a new message that has the same MAC as an existing message.