**Exercise sheet 25 - Network Security**

Alice wants to communicate with Bob. Let (PuA, PrA) and (PuB, PrB) be public-private key pairs of Alice and Bob, respectively. Alice wants to send a message to Bob. In the table, indicate the encryption expression that Alice and Bob would use when Alice sends message M to Bob for each requirement. Use E(Key, Message) and D(Key, Message) to represent encryption and decryption using public and private keys of a message M. Let C be the cipher-text that Bob receives. Also show the decryption at Bob’s end and how you get your message from ciphertext.

|  |  |
| --- | --- |
| 1. Confidentiality only |  |
| 1. Authentication only |  |
| 1. Integrity/cannot be replayed |  |
| 1. Confidentiality and Authentication |  |
| 1. Integrity and authentication |  |