

## SECR0002 Computer Security II

### Asymmetric Crypto System & Hash Function

Bob want to send a message M to Alice. The message is first encrypted with Alice's public key, then signed with Bob's private key and finally produce a message digest using hash function. You have to write a programming to generate the message digest given the following public and private key.

Alice:      Public key: {43, 77}; private key: {7, 77}

Bob:        Public key: {43, 65}; private key: {19, 65}