*Final Project*

The file `RSA.mpl` contains the definitions of Maple procedures for the Rivest/Shamir/Adleman (1976) public key encryption algorithm. Your project is to enhance the `encode` and `decode` procedures to also allow for digital signatures. The calling sequence is

`encode_sign(ClearText, PublicKey, Signature, PrivateSignKeys)`

and

`decode_sign(Code, PrivateKeys, PublicSignKey)`

The procedure `encode_sign` returns a list of two lists of integers, the first one being the same as in the encoding method with a single public key and the second one being the scrambled signature. The procedure `decode_sign` accepts in its *Code* argument a list of two integer lists as is returned by `encode_sign` and returns the *ClearText* followed by the *Signature*. The idea is to instead of encrypting the signature, to **decrypt** the list of (packed) integers with the two *PrivateSignKeys*. Then the decode method **encrypts** the corresponding list of integers, which is the second entry in the *Code* argument, before unpacking them. This authenticates the sent code, since only the sender knows how to decrypt the his signature.