Lab13

1. How would Alice send the message?

Alice would encrypt and send the message via some platform, email, or SMS application. To encrypt the message M\_1, Alice would use the formulae:

E = M\_1^e MOD N

Where E is the resulting encrypted message, e and n using the public key Pu(B).

This would allow Alice to encrypt the message.

1. Let us denote the message Alice sent as M\_3. How would Bob decipher the message?

Bob would again receive the message from Alice through email and decrypt the message using the formulae:

D = M\_3^d MOD N

Where D is the resulting decrypted message, d and n are retrieved from the private key, Pr(B).

1. How would Alice send the message?

To ensure that Bob is the only person that can alter/view the encrypted file Alice would have to encrypt the file using her own public key using the formulae:

E = M\_2^e MOD N

Where E is the resulting encrypted message, e and n using the public key Pu(A).

1. What would Bob do to verify that the message indeed came from Alice?

Bob would have to have Alice private key, Pr(A) to decrypt this. This would mean that Alice is in fact the sender and encrypter of the message if we are able to decrypt with private key, Pr(A).