Approach Note – RSA

I will use following approach for RSA Algorithm –

1. Step 1: Add required libraries like bigint.h, Grand.h etc.
2. Step 2: Generate two random prime variables **p** and **q**.
3. Step 3: Use **p** and **q** to calculate n such that **n = p*q**
4. Step 4: Calculate **Phi** which is equal to **(p-1)*(q-1)**.
5. Step 5: Next I will calculate **e** such that e is less than **n** and is co prime to **Phi**. Also **e** should be a positive integer.
6. Step 6: Since I have calculated **e**, public key is equal to **{e, n}.** Using this public key message will be encrypted as **C = M^e Mod n**.
7. Step 7: Now plaintext message **M** is converted into ciphertext **C**.
8. Step 8: **C** is sent to Bob and now bob will use his private key to decrypt this message.
9. Step 9: To calculate private key we will generate a number **d**, such that **d*e Mod Phi = 1**
10. Step 10: After calculating **d** our private key is **{d, n}.** Using this private key we can decrypt ciphertext **C** as **M = C^d Mod n**.
11. Step 11: Next the plaintext message **M** will be displayed to Bob.