Amrita Vishwa Vidyapeetham, Amritapuri

Department of Computer Science and Engineering

22AIE314 Computer Security

Lab Sheet 4

Public Key Cryptography and Secure Authentication

1. **Implement RSA Algorithm**

   Given:

   Primes: p=13,q=17, Public exponent: e=5, Plain Text: "AMRITA"

   a) Compute n, totient function $\phi(n)$ and private key d.
   b) Encrypt the message using the public key (e,n).
   c) Decrypt the cipher using the private key (d,n)
   d)Verify that decrypted message matches the original.

2. **Implement Diffie Hellman Key Exchange**

   Given:

   - Prime q=5, Primitive root α=2
   - Private keys: A = 3, B = 7

   a) Compute public values of A and B
   b) Find the shared secret key at both ends.