CSE-406

(Computer Security Sessional)

Report on Offline-1

(AES, Diffie-Hellman)

Submitted by:

Tanjeem Azwad Zaman

Roll: 1805006

Dept. of CSE, BUET

Date of Submission:

30.06.2023

Task 1: AES Key Encryption Algorithm

Sample output for a test case

- *Key:*
  In ASCII: BUET CSE18 Batch
  In HEX: 42 55 45 54 20 43 53 45 31 38 20 42 61 74 63 68

- *Plain Text:*
  In ASCII: Can They Do This
  In HEX: 43 61 6e 20 54 68 65 79 20 44 6f 20 54 68 69 73

- *Ciphered Text:*
  In HEX: 80 86 2e 1d 51 7c 4b da 30 18 3d 64 b2 30 21 34
  In ASCII: .↔Q|KÚ0↑=d²0!4

- *Deciphered Text:*
  In HEX: 43 61 6e 20 54 68 65 79 20 44 6f 20 54 68 69 73
  In ASCII: Can They Do This

- *Execution Time Details:*
  Key Schedule Time: 5.4957 ms
  Encryption Time: 331.0122 ms
  Decryption Time: 440.8454 ms

Task 2: Diffie-Hellman Key Exchange

Average Times in milliseconds (Over 20 iterations)

k	Computation Time For				
	p	g	a/b	A/B	Shared Key
128	444.4868	0.167375	1.55326	0.04466	0.05021
192	988.3461	0.28864	2.636145	0.08169	0.08199
256	5546.41	0.477605	5.50888	0.1381	0.12241