CSE-406
Computer Security Sessional
January 2023
Assignment 01
Somonindro Roy
ID: 1805049

Independent Implementation of (128 bit) AES

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']

Key :

In ASCII: BUET CSE18 Batch

In Hex: ['42', '55', '45', '54', '20', '43', '53', '45', '31', '38', '20', '42', '61', '74', '63', '68']

Cipher 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:

Time taken for round key scheduling: 0.007825851440429688 seconds

Time taken for encryption: 0.2793161869049072 seconds

Time taken for decryption: 0.3140530586242676 seconds

Plain Text:

In ASCII : Two One Nine Two

In Hex : ['54', '77', '6f', '20', '4f', '6e', '65', '20', '4e', '69', '6e', '65', '20', '54', '77', '6f']

Key :

In ASCII: Thats my Kung Fu

In Hex: ['54', '68', '61', '74', '73', '20', '6d', '79', '20', '4b', '75', '6e', '67', '20', '46', '75']

Cipher Text :

In Hex: ['29', 'c3', '50', '5f', '57', '14', '20', 'f6', '40', '22', '99', 'b3', '1a', '02', 'd7', '3a']

In ASCII:)ÃP_W ö@"³×:

Deciphered Text:

In Hex: ['54', '77', '6f', '20', '4f', '6e', '65', '20', '4e', '69', '6e', '65', '20', '54', '77', '6f']

In ASCII: Two One Nine Two

Execution time details:

Time taken for round key scheduling: 0.012677431106567383 seconds

Time taken for encryption: 0.2758464813232422 seconds

Time taken for decryption: 0.30531954765319824 seconds

Independent Implementation of Diffie-Hellman

Time-related performance : (Took an average of at least 5 trials)

k	**Computation time for**				
	p	g	a	A	Shared Key
128	0.560698	0.000157	0.067113	4.48226e-05	7.98702e-05
192	0.302098	0.000449	0.013866	8.55922e-05	0.000158
256	8.912881	0.000764	0.477941	0.000152	0.000269