

CS6500 - Network Security Assignment 1: OpenSSL interface and performance analysis

A) AES performance study report

1. Key = 128 bits

AES (time in μ s)

		Key = 128 bits						
		CCM	CFB	CTR	GCM	OFB	XTS	ECB
Mean Block encryption	10 KB	9,22	23,59	3,91	2,66	17,66	4,06	4,06
Mean Block Decryption		9,38	23,44	3,91	2,5	18,13	4,22	3,91
Mean Block encryption	100 KB	92,19	156,25	42,19	23,13	193,75	40,63	42,19
Mean Block Decryption		92,66	312,5	39,06	21,88	190,63	40,63	39,06

2. Key = 256 bits

AES (time in μ s)

		Key = 256 bits						
		CCM	ECB	CFB	CTR	GCM	OFB	XTS
Mean Block encryption	10 KB	12,34	5,47	29,06	5,78	3,44	23,28	5,78
Mean Block Decryption		12,34	5,47	28,28	5,47	3,13	23,44	5,63
Mean Block encryption	100 KB	126,25	56,25	314,06	54,69	31,41	257,81	59,38
Mean Block Decryption		126,25	56,25	318,75	46,88	30	253,13	54,69

B) DES performance study report

DES (time in μ s)

		CBC	CFB	ECB	OFB
Mean Block encryption	10 KB	667,19	689,06	645,31	646,88
Mean Block Decryption		639,06	682,81	637,5	654,69
Mean Block encryption	100 KB	7187,5	7656,25	7343,75	7031,25
Mean Block Decryption		6875	7343,75	7187,5	7343,75

