

Report on Cryptography Algorithms Timing

Asif Shahriar # 1805040

June 2023

1 Algorithms

- Encryption Algorithms
 - AES (Advanced Encryption Standard)
 - RSA (Rivest-Shamir-Adleman)
- Key-exchange Algorithm: Diffie-Hellman

2 AES vs RSA

- Text size: 1908 characters
- Timing unit: milli-seconds

Algorithm	Key scheduling	Encryption	Decryption
AES (symmetric)	2.9992	13504.121	16333.209
RSA (asymmetric)	0.1	6.5236	6.5443

3 Diffie-Hellman with Different Key-sizes

- Text size: 1908 characters
- Timing unit: micro-seconds
- Note: Following timings are average of 5 runs

key-size	p	g	a/b	A/B	shared key	total
128	15103.8	0.0	60.0/20.0	0.0/0.0	0.0/0.0	15183.84
192	93364.52	0.0	80.0/59.98	0.0/20.0	0.0/0.0	93524.5
256	212014.52	20.0	140.0/181.06	0.0/0.0	20.0/0.0	212375.58