Title:	Algorithmic Number Theory and Cryptography
Authors:	Kasera, Abhay (/jspui/browse?type=author&value=Kasera%2C+Abhay)
Keywords:	Algorithmic Number Theory Cryptography Integer Factorization Problem Cryptanalysis of RSA
Issue Date:	4-Sep-2018
Publisher:	IISERM
Abstract:	Primality testing and Integer factorization problem are two widely studied problems in Algorithmic Number Theory. Can we factorize integers in polynomial time is still an unsolved question. However, the Primality testing problem can be solved in polynomial time. RSA is the most widely used Public-key cryptosystem whose security is based on Integer factorization problem. Over past years researchers have studied various attacks on RSA cryptosystem, and it has been concluded that these attacks can be avoided if RSA is implemented securely. In this Thesis we have covered Primality testing algorithms, Factoring algorithms and Cryptanalysis of RSA.
URI:	http://hdl.handle.net/123456789/992 (http://hdl.handle.net/123456789/992)
Appears in Collections:	MS-13 (/jspui/handle/123456789/914)

Files in This Item:

File	Description	Size	Format	
MS13087.pdf (/jspui/bitstream/123456789/992/4/MS13087.pdf)		324.02 kB	Adobe PDF	View/Open (/jspui/bitstream/123456789/992/4/I

Show full item record (/jspui/handle/123456789/992?mode=full)
(/jspui/handle/123456789/992/statistics)