A STUDY OF RSA CRYPTOSYSTEM AND OTHER PUBLIC-KEY CRYPTOGRAPHY

Palash Ranjan Das
MA07C015
2009

This dissertation describes public-key cryptography using Knapsack algorithm, RSA cryptosystem and McEliece scheme. The attacks on RSA algorithm like Brute force attacks, Mathematical attacks and timely attacks. Here cryptographic algorithms are constructed, their working and probable attacks by an intruder are discussed.

This dissertation has three chapters. Chapter one introduces basic concepts to understand the types of algorithm and the public key cryptosystem and the underlying mathematics. Public key cryptography is introduced in chapter two. Knapsack algorithm and RSA cryptosystem are described. Types of attacks on RSA algorithm is analyzed in the final chapter.