2010:4
Självständigt arbete i matematik
Matematiska institutionen
Stockholms universitet

Sara Leufstadius: Asymmetriska krypteringssystem: hur de är konstruerade och vilka matematiska problem de bygger på

Handledare: Rikard Bøgvad

Sammanfattning

I denna uppsats behandlas två moderna krypteringssystem, RSA och ElGamal. Vi visar hur man använder dessa, hur nycklar genereras och hur man sedan krypterar och dekrypterar meddelanden. För båda systemen gäller att de bygger på var sitt svårlöst matematiskt problem, i RSA:s fall handlar det om primtalsfaktorisering och för ElGamal är det fråga om det diskreta logaritmproblemet. Utifrån respektive problem konstrueras en envägsfunktion som är lätt att beräkna åt ena hållet, men om man däremot vill finna dess invers är det i praktiken omöjligt om man inte också har tillgång till extra information, vilken gör beräkningen av inversen genomförbar. Vi studerar också några olika algoritmer och metoder för att lösa de två problem som systemen bygger på. Till sist tar vi upp något som berör båda krypteringssystemen, nämligen hur man avgör om ett tal är ett primtal.