Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 8b: Donderdag 29 April 2004

US nommer: _____ Voorletters: _____ Van: _____

Klasnotas en/of Programmatuur Toegelaat

Gebruik *Pollard se algoritme* en die *gewysigde Euklidiese algoritme* om die betekenis van die kriptoteks $y = 5\,564$ te ontrafel, wat met behulp van die RSA–sisteem aan 'n gebruiker met publieke sleutelgetalle $n = 6\,887$ en $e = 4\,567$ gestuur is. Toon die afvoer in elkeen van die stappe van elk van die algoritmes, motiveer u argumente en sit u algemene benadering om die RSA–sisteem te breek, duidelik en sinvol uiteen.