Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 7b: Donderdag 22 April 2004

US nommer: _____ Voorletters: _____ Van: _____

Gebruik van Rekenaarprogrammatuur en van Klasnotas word toegelaat

Die kriptoteks (253, 1730) is deur middel van die ElGamal publieke sleutel kriptosisteem gevorm, en die publieke sleutelparameters van die regmatige ontvanger van die boodskap word gegee deur $\alpha = 716$, $\beta = 2\,373$ en $n = 2\,789$. Breek die sisteem deur middel van Shanks se algoritme en dekripteer sodoende die kriptoteks. Motiveer u werking volledig. [Wenk: 'n bloklengte–protokol van 4 syfers (2 karakters) is gebruik.]