Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 8a: Donderdag 29 April 2004

US nommer: _____ Voorletters: _____ Van: _____

Die Gebruik van Klasnotas en/of Programmatuur word Verbied

Verduidelik breedvoerig hoe Persoon A (met publieke sleutelgetalle n_A, e_A en geheime sleutelgetalle p_A, q_A, d_A) 'n *geheime, digitaal ondertekende* boodskap met behulp van die RSA–sisteem aan Persoon B (met publieke sleutelgetalle n_B, e_B en geheime sleutelgetalle p_B, q_B, d_B) sal stuur, en wat persoon B sal doen om die inhoud van die boodskap te herwin en te verseker dat Persoon A wel die regmatige sender van die boodskap is (m.a.w. die egtheid van die handtekening verifieer).