

Serious Cryptography, 2nd Edition

A Practical Introduction to Modern Encryption

by Jean-Philippe Aumasson

Errata updated to print 1

Page	Error	Correction	Print corrected
198	<pre>sage: d = xgcd(e, phi); d 15417970063428857</pre>	<pre>sage: d = xgcd(e, phi)[1] ; d = mod(d, phi) 11417851791646385</pre>	Pending
199	<pre>sage: y = power_mod(x, e, n); y 19048323055755904</pre>	<pre>sage: y = power_mod(x, e, n); y 17129109575774132</pre>	Pending
276	You can then express a qubit's state as $\alpha 0\rangle + \textcircled{\alpha} 1\rangle, \dots$	You can then express a qubit's state as $\alpha 0\rangle + \beta 1\rangle, \dots$	Pending