

To me, To you: The Three Pass Protocol

Dr Paul Truman
(Keele University)

Monday 4 December 2017, 6.30pm
(Refreshments from 6.00pm)

Mitchell & Kenyon cinema,
Foster Building,
UCLAN, Preston

Abstract

All symmetric ciphers (in which the same key is used to encrypt and decrypt the message) suffer from a common problem: how do the users agree securely upon a key? The Three Pass Protocol allows users to communicate without the need to exchange keys. We will discuss this counter-intuitive idea, explore how it can be implemented, and illustrate how it paves the way towards public key cryptography.

About the speaker

Paul Truman, graduated from the University of Oxford in 2005 and studied for a PhD in algebraic number theory at the University of Exeter. He left Exeter in 2010 to go to Keele University. His research interests are in algebra and number theory, specifically the Galois module structure of algebraic integers



For further information, please contact Danielle Bewsher DBewsher@uclan.ac.uk
or Margaret Eastwood margareteastwoodimanw@gmail.com

No charge is made to attend meetings. Non-IMA members are welcome.