UNIVERSITÀ DEGLI STUDI DI MILANO

SCUOLA DI DOTTORATO IN FISICA
ASTROFISICA E FISICA APPLICATA

2011/2012 Physics Colloquia

// Is there a perfect cypher? //

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of our civilisation.
Over the centuries many ingenious methods of secret communication have been developed, only to be matched by the ingenuity of code-breakers.
As the result, the quest for a perfect, unbreakable, cipher, had been declared a futile pursuit. That is, until recently!
Surprisingly, a combination of quantum physics and cryptography promises to dash the hopes of would-be eavesdroppers, perhaps for good.
Code-makers, it seems, may have beaten code-breakers at last.
In my talk I will focus on the quest for perfect secrecy. I will describe how people tried to protect communication in the past, how it is done today, and I will speculate how it may be done in the future.
I will explain how, using quantum phenomena, physicists managed to design and to implement a system which is regarded to be unbreakable.
RECOMMENDED READING: Semi-popular article titled "Less reality, more security" available at http://www.arturekert.org/Site/Varia.html.
Abbreviated version published in Physics World, September 2009.

28 FEB 2012

Artur Ekert
University of Oxford, U.K.

Is there a perfect cypher?

Gli incontri si terranno alle **ore 15:00**
nell'**aula A** del **DIPARTIMENTO DI FISICA**
via Celoria 16 | 20133 MILANO | Tel. +39 02 50317740
http://phd.fisica.unimi.it | phd@fisica.unimi.it

progetto grafico:
roberto perego | www.nonacaso.it