



UNIVERSITÀ DEGLI STUDI
DI TRENTO

Facoltà di Scienze MM.FF.NN.
Dipartimento di Matematica

UNIVERSITÀ
DEGLI STUDI
DI TORINO

ALMA UNIVERSITAS
TAURINENSIS



Crittografia a chiave pubblica: oltre RSA

Questo corso di crittografia a chiave pubblica è stato realizzato grazie ad un'iniziativa congiunta del Dipartimento di Matematica dell'Università di Torino e del Dipartimento di Matematica dell'Università di Trento.

Venerdì 13 maggio 2011

– Dipartimento di Matematica – Università di Torino

9:00 – 09:45	Introduzione alla crittografia, Diffie-Helman e RSA <i>Dott. Daniele Giovannini, Università di Trento</i>
09:45 – 10:20	La crittografia a curve ellittiche (ECC) <i>Dott. Emanuele Bellini, Università di Trento</i>
10:20 – 10:45	Curve iperellittiche <i>Dott. Stefania Vanzetti, Università di Torino</i>
<hr/>	
10:45 – 11:00	<i>Coffee break</i>
<hr/>	
11:00 – 11:45	Applicazioni reali di RSA e altri sistemi <i>Dott. Renato Sabbatini, AlphaOrionis</i>
11:45 – 12:15	Altri crittosistemi alternativi <i>Dott. Emanuela Orsini, Università di Pisa</i>
<hr/>	
12:15 – 12:30	<i>Coffee break</i>
<hr/>	
12:30 – 13:00	Attacchi e sicurezza dei sistemi, con paragoni e conclusioni <i>Prof. Massimiliano Sala, Università di Trento</i>