U.S.T.H.B.
Faculté de Mathématiques.

Programme des cours
du professeur Michel WALDSCHMIDT.
Du 05 au 09 Mai 2013.

Dimanche 5 Mai 2013	**9H30 - 11H00.**	**13H30 - 15H30.**
	Introduction à la cryptographie.	Structure des groupes finis; cas du groupe multiplicatif des unités modulo n; application au protocole RSA.
Lundi 6 Mai 2013	**10H – 11H30.**	**13H30 – 15H30.**
	<u>Conférence.</u> Codes correcteurs d'erreurs.	Structure des groupes de type fini; applications : théorème des unités de Dirichlet, groupe de Mordell-Weil d'une courbe elliptique ou d'une variété abélienne.
Mardi 7 Mai 2013	**9H30 - 11H00.**	**13H30 – 15H30.**
	Cryptosystèmes à clés publiques. Cryptosystème RSA.	Algorithme d' El Gamal. Protocole de Diffie-Hellman.
Mercredi 8 Mai 2013	**9H30 - 11H00.**	**13H30 – 15H30.**
	Cryptosystème de Rabin. Problème du sac à dos.	Cryptosystème de Merkle-Hellman.
Jeudi 9 Mai 2013	**9H00 - 11H00.**	**Après-midi**
	Séance de travail avec les Doctorants.	