



crypt@b-it 2007
24-28 September 2007,
b-it, Bonn, Germany.



This summer school on cryptography offers undergraduate and graduate students and researchers the opportunity to crypt a bit. It provides acquaintance and interaction in an intellectually stimulating and informal atmosphere in pleasant surroundings.

Speakers

- Joachim von zur Gathen , b-it Bonn,
- Frank Niedermeyer, BSI Bonn,
- Pascal Paillier, Cryptography & Innovation, Security Labs, Gemalto,
- Gadiel Seroussi, MSRI Berkeley.

Programme

	Monday	Tuesday	Wednesday	Thursday	Friday
0900-1030	Pascal Paillier, Security reductions for asymmetric systems				
1100-1230	Gadiel Seroussi, Elliptic curve cryptography				
	Lunch break				
1400-1530	Tutorials and exercises	Frank Niedermeyer, The Enigma machine	Excursion	Tutorials and exercises	
1600-1730	Tutorials and exercises				

Application

- The intended audience are undergraduate and graduate students as well as postdocs and researchers who work in the area or at least have a basic knowledge.
- The event is for free. Each participant will contribute 25€ (for refreshments during the breaks) plus the fare (for those who take part in the excursion).
- Application: **Apply online(!) before Thursday 30 August 2007.**
- Webpage: <http://www.b-it-center.de/> →Groups →computer security
→Summer school: crypt@b-it 2007

Contact Information

For questions, further information, or suggestions, please send an email to cryptabit@bit.uni-bonn.de