# BIRS Workshop
# Number Theory Inspired by Cryptography
# 6-10 November, 2005

## MEALS

Breakfast (Continental): 7:00 - 9:00 am, 2nd floor lounge, Corbett Hall, Sunday - Thursday
Lunch (Buffet): 11:30 am - 1:30 pm, Donald Cameron Hall, Sunday - Thursday
Dinner (Buffet): 5:30 - 7:30 pm, Donald Cameron Hall, Saturday - Wednesday
Coffee Breaks: As per daily schedule, 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each lunch and dinner.**

## MEETING ROOMS

**All lectures are held in the main lecture hall, Max Bell 159.** *Please note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155-159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.*

## Sunday, 6 Nov.

8:30 - 9:00 Introduction to BIRS by Brenda, the BIRS Station Manager

9:00 - 9:45 Jonathan Sorenson, *Upper and lower bounds on the distribution of smooth numbers*

9:50 - 10:20 Denis Charles, *Signatures for Network Coding*

10:20 - 10:45 Coffee Break

10:45 - 11:30 Edlyn Teske, *Generating elliptic curve parameters for pairing-based cryptography*

11:30 - 1:30 Lunch

1:00 - 2:00 A guided tour of the Banff Centre

1:30 - 5:30 Free Afternoon for discussions

3:20 - 3:50 Coffee Break

5:30 - 7:30 Dinner

7:40 - 8:30 Dan Bernstein, *Compressing RSA/Rabin keys*

## Monday, 7 Nov.

9:00 - 9:45 John Friedlander, *A Problem in combinatorial number theory*

9:50 - 10:20 Allison Pacelli, *High n-Rank in Class Groups of Global Fields*

10:20 - 10:45 Coffee Break

10:45 - 11:30 Pedro Berrizbeitia, *Eisenstein Reciprocity Law, Gaussian Sums and Application to Primality Testing*

11:30 - 1:30 Lunch

1:45 - 2:30 Gerhard Frey, *Arithmetic aspects of Brauer groups and applications to discrete logarithms*

2:35 - 3:20 Samuel Wagstaff, *Square form factorization*

3:20 - 3:50 Coffee Break

3:50 - 4:35 Qi Cheng, *An efficient keyless number-theoretic hash*

4:40 - 5:25 Kristin Lauter, *New constructions of cryptographic hash functions*

5:30 - 7:30 Dinner

## Tuesday, 8 Nov.

9:15 - 10:00 Florian Luca, *Structure of Groups of Points on Elliptic Curves*

10:00 - 10:25 Coffee Break

10:25 - 11:10 Nicolas Theriault, *Double large prime index calculus for hyperelliptic curve cryptosystems*

11:15 - 11:30 Group Photo

11:30 - 1:30 Lunch

1:30 - 5:30 Free Afternoon for discussions

3:20 - 3:50 Coffee Break

5:30 - 7:30 Dinner

7:40 - 8:30 Francois Morain, *New improvements to the SEA algorithm*

## Wednesday, 9 Nov.

9:00 - 9:45 Tanja Lange, *Efficient computation of pairings on non-supersingular hyperelliptic curves*

9:50 - 10:20 Isabelle Dechene, *Generalized Jacobians in cryptography*

10:20 - 10:50 Coffee Break

10:50 - 11:35 Renate Scheidler, *The real model of a hyperelliptic curve*

11:35 - 1:30 Lunch

1:30 - 5:30 Free Afternoon for sightseeing

5:30 - 7:30 Dinner

## Thursday, 10 Nov.

9:30 - 10:15 Kumar Murty, *Ramanujan Graphs and Isogenies of Elliptic Curves*

10:15 - 10:45 Coffee Break

10:45 - 11:30 Free Morning for discussions

11:30 - 1:30 Lunch