GC Cryptography Student Seminar Grant Proposal

As the use of computer in modern life become more and more widespread, the need for computer security also increase. Cryptography, therefore, becomes an attractive field of study, not only for computer scientists but also for mathematicians whose knowledge is fundamental to the underlying principles of cryptography.

Seeing the need for communication between the disciplines and the lack of an informal, student level seminar, the GC Cryptography Student Seminar was formed. We have been meeting weekly since Fall 2010, attracting speakers from both the Mathematics and Computer Science departments. We try to keep the talks at a student level, accessible to both mathematicians and computer scientists. Because of this, we have members ranging from undergrads from various CUNY campuses to PhD candidates at the Graduate Center.

Due to the novelty of the field of Cryptography, various ideas and applications are being explored. For example, this Fall 2012 semester, we have prepared talks about different cryptosystems, key exchange protocols, digital signatures, secret sharing schemes among other topics. Our website [https://sites.google.com/site/gccryptostudents/] announces up-coming talks and also provide slides and/or relevant papers ahead of time so members as well as non-members can come prepared.

Our faculty organizer, Professor Dr. Delaram Kahrobaei, is both a computer scientist and a mathematician who has taught Cryptography classes at the Graduate Center, given talks to international conferences and published extensively on the subject. More than that, she is interested in mentoring and developing collaborations among female faculty and Ph.D students. Thanks to that, a number of our seminar's core members are female students at the Graduate Center, and we are hoping to attract more.

This semester, we are meeting from 1:00-2:30pm every Friday in room 8405. Because the seminar happens during lunch time, we are trying to provide a small quantity of refreshment that includes pizza and juice or soda. Including the seminars organizers, the seminar regularly is attended by an average of ten students. For this reason we are requesting $25 per week for buying two cheese pizzas, and soda or juice. We also anticipate that the refreshment will attract more participants to the seminar.

The seminar will have six talks after the 10/12/2012. These talks are free and open to public, therefore we are seeking sponsorship from the DSC as a Start-Up in the Fall semester for refreshments in the total of $150. Please see the attached sample flyer showing DSC sponsorship and our proposed line item budget.

Thank you very much for your considerations.

Mock Line Item Budget for the Cryptography Student Seminar Project

Line Item	**Cost**
Food and Drinks	
Pizza	$120
Assorted drinks	$30
Total	**$150**

Break Down of Expenditures for the Remainder of the Semester

10/19/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
10/26/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
11/9/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
11/16/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
11/30/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
12/7/12	
Pizza	$20
Soda or Juice	$5
Sub-total	*$25*
Gran total	**$150**

GC Cryptography Student Seminar

THE GRADUATE CENTER

THE CITY UNIVERSITY OF NEW YORK

365 FIFTH AVENUE AT 34TH STREET

NEW YORK CITY

FRIDAY, SEPTEMBER 28, 2012

1:00 P.M.-3:00 P.M.

Room 8405

Student Organizers:

Ha T. Lam

Bianca Sosnovski

Faculty Organizer:

Dr. Delaram Kahrobaei

FREE and OPEN to the Public

Cosponsored by the PhD Program in Mathematics and Computer Science, CUNY Graduate Center and by the Doctoral Student Council

For more information, please visit our website:
https://sites.google.com/site/gccryptostudents/

Yunqi Xue

Computer Science Department, GC, CUNY

“Ron was wrong, Whit is right”

based on the paper by Lenstra, Hughes et. al.

Abstract: “We performed a sanity check of public keys collected on the web. Our main goal was to test the validity of the assumption that different random choices are made each time keys are generated. We found that the vast majority of public keys work as intended. A more disconcerting finding is that two out of every one thousand RSA moduli that we collected offer no security. Our conclusion is that the validity of the assumption is questionable and that generating keys in the real world for “multiple-secrets” cryptosystems such as RSA is significantly riskier than for “single-secret” ones such as ElGamal or (EC)DSA which are based on Diffe-Hellman. ”
(from the paper “Ron was wrong, Whit is right” by Lenstra, Hughes et. al.)