Concise abstract

Objective: Study theory & implementation of new cryptographic systems, specifically...

The objective of this research is to open new possibilities or better understand subjects in the field of non-commutative group cryptography. The topic includes the algorithms used in enciphering and deciphering private messages using public key protocol, especially with the help of properties of some nonabelian groups, as well as the general security of those methods and possible weaknesses of them. My personal goal is to

(*)

Cryptography is... Briefly explain that "public key crypt. allows us to, for example, send information securely online"

Coursework

explain

This topic has very close relation with abstract algebra, as it deals heavily with properties of groups and their elements. I took Math 307 (abstract algebra), which is the basis of the structure in group based cryptology. Moreover, Math 430 is the following course that focuses on rings while the first course focuses on groups. While group-based cryptography is centered around group theory and its applications, the latter course should aid me in some way since rings are similar to groups in some extent.

CS course?

GOALS: 10 weeks of summer research, methodology for those goals

Interesting? Exciting? Unique?

The field of cryptology played a crucial role in human history, dating back to some 3,000 years back. However, it had been rarely ever openly studied as a subject, generally because the subject was indeed crucial in information security. However, now cryptology is an active field of study that inspires some question in algebra as well. More importantly, the protocol used nowadays seems secure, but the improvement of devices could make weaknesses in them by breaking the decrypted messages by brute force method. Thus, we need to look forward and develop even more secure methods, and cryptosystem based on nonabelian groups offers a considerable possibility. My research will contribute in better understanding the possible basis groups for some cryptosystems, which could lead to securer system for information security.

- Review of latest research, e.g.) techniques, etc.
- Determine the Constraint appropriate groups to use as well as design the appropriate algorithms

"Pilot research"

Citations?

Long-term Goals

This research is the start of what I wanted to do personally in the future. I had much interest on the concept of abstract algebra and cyber security, and group-based cryptology is where the two subject coincide. As the field is relatively new and very active, I should get a new point of view on the subject; even if I do not get any significant results, the information that I would gather during the research will certainly provide me with a strong background to begin.

(*): Public key cryptography is ... allows the secure transmission of data online ---

With the possible invention of [ ], the current methods could be vulnerable to [attacks].

LOOK @ summaries from 2016, 2015, etc., winners of this fellowship.

My research will involve the analysis and implementation of cryptography based on nonabelian groups, which are potentially secure under such attacks.

Don't "state". DEMONSTRATE.