RESEARCH STATEMENT

KATHRYN TRUMAN

My research is in the general area of Algebra and Number Theory, and more specifically Cryptography. A cryptosystem is used when a person, Alice, wants to send a message securely to another person, Bob. In a public key cryptosystem, Alice uses Bob's public key to create her encrypted message, which she sends to Bob. Bob can then use his private key to decrypt and read Alice's encrypted message. No one else can decrypt Alice's message without knowing Bob's private key. An advantage of public-key cryptography is that Bob publishes one public key for all people who send him messages, and this makes key distribution easier.

In my research I study the ring-based public key cryptosystem NTRU, where the message, the private key, and the public key are elements of an integral group ring modulo a prime number. The version with the most commercial success has been the commutative version, which uses the group ring of a cyclic group. This ring can also be thought of as a quotient of a polynomial ring. There is much current work on this system (see www.ntru.com). There is also a non-commutative version of the system which leads to very interesting mathematics. Coppersmith gave an attack that breaks the system over the group ring of the dihedral group, but some of the most interesting phenomena do not occur in this case. My work generalizes Coppersmith's attack to group rings of other meta-cyclic groups, where the interesting phenomena do occur. My attack can be expressed through the theory of matrix representations of groups.

The attack uses a commutative subring of the group ring and modules over this subring. Using techniques from algebraic number theory and representation theory, I show these modules are principal over the subring. Using these modules and the properties of the system, I am able to produce a substitute for the private key which allows for the creation of a decryption function.

Details: Let G be generated by X and Y with the relations $X^N = 1$, $Y^\ell = 1$ and $YXY^{-1} = X^k$ for a suitable k. Let R_0 be the commutative subring of $R = \mathbb{Z}[G]$ consisting of elements that commute with Y. To set up the system we also need integers p and q with p much smaller than q. For his public key Bob chooses a suitable random $w \in R$ and a random $f \in R_0 \pmod{q}$. He next computes $F \in R_0 \pmod{q}$, the inverse of $f \pmod{q}$. Bob's public key is $h = F * pw * f \pmod{q}$, and f, w, and F are kept private. If Alice wants to send a message $m \in R \pmod{q}$ to Bob, she chooses suitable random ϕ, ϕ', and $\psi \in R_0$.

She next computes $\Psi \equiv \psi \pmod{p}$. The encrypted message is the pair (e, E) where

$$e \equiv \phi * h * \phi' + \psi \pmod{q}, \qquad E \equiv m + \Psi * h \pmod{q}.$$

To decrypt the message, Bob computes

$$a \equiv f * e * F \pmod{q}$$

and then reduces this modulo p to get Ψ, which allows him to compute

$$m \equiv E - \Psi * h \pmod{q}.$$

To break the system it is only necessary to know h. Define the modules R_ζ over R_0 as the set of elements α in R such that $Y * \alpha = \zeta\alpha * Y$ where ζ is an ℓ^{th} root of unity. It is then possible to create a function θ so that $\theta(e) \pmod{p}$ will produce Ψ, for any encrypted message (e, E), allowing the message m to be read. The function θ needs to be R_0 linear and take R_ζ into itself for each ζ. To create θ we need a w' that works like w, and there is a simple method for finding w'. After doing so we then rely on matrix representations of groups and linear algebra to find θ. The calculations for finding θ are easily done in Maple and MAGMA.

Continued Research: I am working on extending non-commutative NTRU to group rings of groups with more than two generators. Also, I am interested in trying to unify non-commutative and commutative NTRU. The non-commutative system does not simplify to the commutative system if G is a commutative group, but it is very similar. Developing a non-commutative system that reduces to commutative NTRU would be very interesting. I have spoken on braid group cryptography and would like to continue to investigate other non-commutative cryptosystems.

Undergraduate Research: Undergraduates often are very interested in number theory and its applications to cryptography. There are numerous opportunities to do research with undergraduates in cryptography since there are many cryptosystems that require only basic abstract algebra, linear algebra, or number theory. I am very interested in exploring new areas as well as continuing to work on cryptosystems like NTRU with undergraduates. Students with programming experience could help develop algorithms and computer programs to implement and break cryptosystems. In my experience at a summer REU I found the mix of computer programs and theoretic mathematics exciting.