Independent Study
Undergraduate Research
REU

Chris Christensen
Northern Kentucky University
Northern Kentucky
NKU: A “Directional” University

- Students enrolled, fall 2007: 14,807.
- Undergraduates: 12,725.
- Full-time: 9,850, part-time: 4,957.
- From Kentucky: 10,196
- From Boone, Campbell, or Kenton County: 8,248.

- 1,400 residence hall spaces.
Mathematics and Statistics

- Nineteen tenure track faculty.
- 4-course teaching load.
- 5 doing undergraduate research.
- 120 majors.
- 28 graduates last year.
Undergraduate Research
Beyond the usual classroom relationship.

Students seeing faculty as researchers rather than teachers.

Faculty seeing students as colleagues.
Beyond the Usual Classroom Teaching

- Independent study classes.
- Class projects.
- Contest participation.
- Sophomore seminar.
- Capstone experience.
- Student travel.
- Disciplinary clubs.
STUDENTS
- Money.
- Preparation for graduate school or employment.
- Interesting problem.
- Travel.
- It’s fun.
- Recognition.
- Develop a closer relationship with faculty.

FACULTY
- Money? Travel?
- Encouragement by chair.
- It’s fun (at least the actual research).
- It’s our job.
Making It Happen

- Encourage research during the academic year.
- Encourage REU participation. And, follow up on it.
- Encourage summer research. Money!
Summer Research

- REU participation.
- Summer Fellowship.
What makes it happen on-campus?

Money for students!
Requires a student-authored proposal.

Student receives a summer stipend.

Faculty solicit students or students select faculty based upon faculty interests.
What makes it happen for REU participation?

Encouragement!
Presentations in the Department

- Student presentations at clubs.
- Sophomore seminar.
- Student presentations in classes.
Three-day Celebration in April

- Student presentations.
- Poster session.
- Performances and exhibitions.
Regional and National Conferences

- Regional conferences: Miami University Mathematics and Statistics Conference. Western Kentucky University Mathematics Symposium, Rose-Hulman Undergraduate Mathematics Conference, KYMAA.
- National Conference: MathFest and Joint Mathematics Meetings.
Finding Problems

Quasi p-groups
Cryptology
Quasi $p$-group: a group that is generated by elements whose orders are powers of $p$, a prime.

These results formed Ben’s Honors Thesis and were presented at Miami University Mathematics and Statistics Conference (2), Rose-Hulman Undergraduate Mathematics Conference (3), Western Kentucky University Mathematics Symposium, KYMAA (2), University of Dayton colloquium, and were published in two articles in the Rose-Hulman Undergraduate Mathematics Journal.
Summer 2004: Jesse continued the work of Ben. These results were presented at the Miami University Mathematics and Statistics Conference, 2004, the Western Kentucky University Mathematics Symposium, 2004, and the Joint Mathematics Meetings in Phoenix, 2005, the Rose-Hulman Undergraduate Mathematics Conference, 2005, and NKU’s Celebration of Research and Creativity, 2005.
Joe Gastenveld, Summer 2005 and summer 2006. Joe continued the work of Ben and Jesse.

These results were presented at the Miami University Mathematics and Statistics Conference, 2005, the Western Kentucky University Mathematics Symposium, 2005, the Joint Mathematics Meetings in San Antonio, 2006, the Kentucky Section of the MAA, 2006.
Joe’s results appeared in the Spring 2008 Pi Mu Epsilon Journal, 12(8), pp. 455 - 458 as “Extensions that Yield Quasi $p$-Groups.”

Joe’s paper received a Richard V. Andree Award for being one of the best undergraduate-written articles to appear in the 2008 issue of the Journal.

---

**Theorem 6** A finite group $G$ is a quasi $p$-group if and only if $G/\Phi(G)$ is a quasi $p$-group.

**Proof:** If $G$ is a quasi $p$-group, then $G/\Phi(G)$ is a quasi $p$-group because it is a homomorphic image of $G$.

Assume that $G/\Phi(G)$ is a quasi $p$-group. By way of contradiction, assume that $G$ is not a quasi $p$-group. This implies that $p(G)$ is a proper normal subgroup of $G$. By [7], (2.28) $p(G)\Phi(G)$ is a normal subgroup of $G$. We claim that $p(G)\Phi(G) \neq G$. If it were true that $p(G)\Phi(G) = G$, then (because $\Phi(G)$ consists of non-generators) we would have that $G = p(G)$ (i.e., $G$ would be a quasi $p$-group) and we have assumed that this is not the case. Therefore, $\Phi(G) \leq p(G)\Phi(G)$ and $p(G)\Phi(G)$ is a proper normal subgroup of $G$. Then $p(G)\Phi(G)/\Phi(G)$ is a normal subgroup of $G/\Phi(G)$.

Notice that $\frac{G}{p(G)\Phi(G)} \cong \frac{G}{[p(G)]\Phi(G)}$. Consider the order of the right-hand side. So $|\frac{G}{p(G)\Phi(G)}| = \frac{|G|}{|p(G)\Phi(G)|}$. By [10] (2.20), $|p(G)\Phi(G)| = \frac{|p(G)|\Phi(G)}{|\Phi(G)|}$.

So, $|\frac{G}{p(G)\Phi(G)}| = \frac{[p(G)]\Phi(G)}{|p(G)|\Phi(G)} = \frac{|p(G)|\Phi(G)}{|p(G)|\Phi(G)} = \frac{|p(G)|\Phi(G)}{|p(G)|\Phi(G)}$, which is prime to $p$. This is a contradiction because we have a homomorphic image of $G/\Phi(G)$ that has order prime to $p$. Therefore, the assumption that $G$ is not a quasi $p$-group is false.

QED
Alex Kuhl and Nick Hoffman
Fall 2006. Nick developed his final class project – a description of the IDEA encryption algorithm -- from the Spring 2005 Cryptology class into a simplified version of the algorithm that exhibits the methods of the algorithm but is easy enough to be done by hand calculation. Nick’s simplified IDEA algorithm can be used by students to develop understanding of the algorithm. Nick’s paper “A Simplified IDEA Algorithm” appeared in the April 2007 issue of Cryptologia. For this paper, Nick won Cryptologia’s Undergraduate Student Paper Competition Prize for 2007.
Spring 2007. Alex followed up on an idea from the Spring 2005 Cryptology class and wrote a paper about the computer reconstruction he did of the lost catalog of rotor settings developed by the Polish mathematician Rejewski in the 1930s. Rejewski’s catalog was used by the Polish codebreakers to attack the German Enigma encryption machine.

Alex’s paper “Rejewski’s Catalog” appeared in the October 2007 issue of Cryptologia.

For this paper, Alex was awarded Cryptologia’s Greg Mellen Memorial Scholarship Prize for 2007.

<table>
<thead>
<tr>
<th>Disjoint Cycle Structure (AD)(BE)(CF)</th>
<th>Number of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>(13 13)(13 13)(13 13)</td>
<td>1771</td>
</tr>
<tr>
<td>(12 12 1 1)(13 13)(13 13)</td>
<td>898</td>
</tr>
<tr>
<td>(13 13)(13 13)(12 12 1 1)</td>
<td>866</td>
</tr>
<tr>
<td>(13 13)(12 12 1 1)(13 13)</td>
<td>854</td>
</tr>
<tr>
<td>(11 11 2 2)(13 13)(13 13)</td>
<td>509</td>
</tr>
<tr>
<td>(13 13)(12 12 1 1)(12 12 1 1)</td>
<td>494</td>
</tr>
<tr>
<td>(13 13)(13 13)(11 11 2 2)</td>
<td>480</td>
</tr>
<tr>
<td>(12 12 1 1)(13 13)(12 12 1 1)</td>
<td>479</td>
</tr>
<tr>
<td>(13 13)(11 11 2 2)(13 13)</td>
<td>469</td>
</tr>
<tr>
<td>(12 12 1 1)(12 12 1 1)(13 13)</td>
<td>466</td>
</tr>
<tr>
<td>(13 13)(10 10 3 3)(13 13)</td>
<td>370</td>
</tr>
<tr>
<td>(13 13)(13 13)(10 10 3 3)</td>
<td>360</td>
</tr>
<tr>
<td>(10 10 3 3)(13 13)(13 13)</td>
<td>358</td>
</tr>
<tr>
<td>(13 13)(13 13)(9 9 4 4)</td>
<td>315</td>
</tr>
<tr>
<td>(9 9 4 4)(13 13)(13 13)</td>
<td>307</td>
</tr>
</tbody>
</table>
REU Proposal

NKU and UC.
Partnership

NORTHERN KENTUCKY UNIVERSITY

UNIVERSITY OF CINCINNATI
Proposal Strengths

- NKU’s experience with undergraduate research and emphasis on teaching undergraduates.

- UC’s strength with mathematical research in cryptology.
Foundation for the Proposal

- Student presentations at meetings.
- Student papers.
- UC faculty research.
8 weeks – mid-June until mid-August.
6 participants.
Live in apartments on NKU campus and work in NKU Department of Mathematics.
Mentored by two UC graduate students.
Mentored by Jintai Ding of UC Department of Mathematical Sciences.
Offers

- $3000 stipend.
- Travel to and from NKU.
- Housing and meals on NKU campus.
- Travel money for a conference.
Selection of Participants

Creativity and patience

Previous research.

Other school’s students.

Other NSF concerns.
REU people
From

- NKU
- University of Wisconsin
- Transylvania University
- Taylor University
- University of Michigan
- University of Texas
Problems

- KeeLoq
- SMS4
- Simplified AES
- DES
Our REU emphasized experimental mathematics – computer experiments using Magma.
A Day in the Computer Lab
What can be done in 8 weeks?

- Research versus teaching in the REU.
- Working at a distance after the REU.
- When to write.
- Encourage presentations.
Jeremy Erickson completed his thesis for his computer science major.

Brian Nixon put together a package of Magma programs the Year Two participants will use.

Amber Rogers spoke about KeeLoq and algebraic cryptanalysis at the JMM.

Sean Simmons is revising an article about S-AES for Cryptologia.
Other REU Goals

Encourage students to enter graduate school in mathematics.

Learn to write mathematics.

Present results.

Submit a paper?
REU

Plans for Year Two.
Select participants early.

More writing and presentation during the REU.

An undergraduate mentor.
Keep in touch with participants.

Encourage presentations and papers.
Year Three and Beyond
Encourage REU participants to:

Present on-campus and at meetings.

Write a paper, if appropriate.