ASU College of Liberal Arts & Sciences
ARIZONA STATE UNIVERSITY

PHYSICS FLASH

News from the Department of Physics ~ July 2009

IN THE NEWS…

The US Department of Education has funded a Graduate Assistance in Areas of National Need or GAANN proposal written and submitted by ASU Physics Regents' Professor Otto Sankey and Professor Tim Newman, Director of the Center for Biological Physics.

The award will fund four graduate student fellows for three years. Students will be studying several issues within biological physics. The award serves as a powerful recruiting tool for top graduate students in biological physics and will be used to fund both new and continuing students.

Receipt of this grant is a reflection on the reviewers assessment of the quality of ASU Physics graduate program as well as the university in general.

Congratulations to ASU Physics professor Lawrence Krauss on who was recently honored by the Center for Inquiry's 12th World Congress on Science, Public Policy and the Planetary Community for his "Scholarship in the Public Interest." The award recognizes his involvement in science and society issues as well as his public outreach efforts. Click HERE for more details.

Krauss also recently participated in several sessions of the World Science Festival held in New York this past June. The annual festival seeks "to cultivate and sustain a general public informed by the content of science." Participants included scientists, journalists, philosophers, historians, performing artists, and students in a week-long series of eclectic discussions.

MNS program impacts high school physics classrooms through teacher training

Now entering its ninth year, the Master of Natural Science program in ASU Physics continues its mission to provide junior high and high school physics teachers with the professional development necessary to keep their physics classrooms engaging and relevant. The program, which began in 2001, grew from a series of modeling workshops designed to help high school teachers prepare to teach physics effectively.

Graduate students in the Master of Natural Science program explore and discuss techniques to improve content delivery in high school physics classrooms.

There are approximately 23,000 high school physics teachers in the U.S., two-thirds of whom did not major in physics or physics education. The most common degree for high school science teachers is biology. Teachers are often recruited to teach across the science curriculum including earth science, biology, physics, chemistry, and others. While that may be an efficient use of resources, it does little to ensure that students are getting the latest information or that teachers are using effective physics pedagogical methods.

Intensive summer modeling workshops were designed with these teachers in mind as well as for PhDs in physics entering the classroom for the first time. The workshops eventually evolved into an interdisciplinary graduate program—the Master of Natural Science (MNS) degree in physics teaching.

With nearly 200 students enrolled annually, the program has been recognized as a ground-breaking achievement for physics education in the United States. In its 2005 report, the North Central Accrediting team noted that "There appears to be no comparable

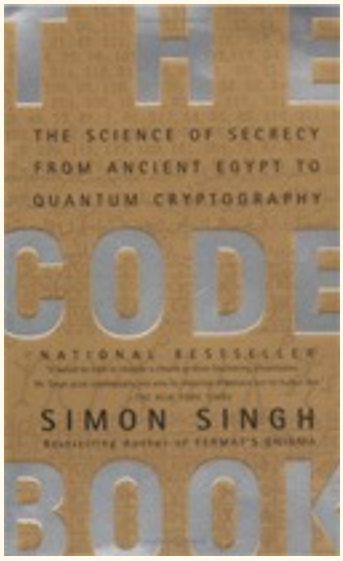
(Continued on Page 3)

BOOK REVIEW:

The Code Book

by Simon Singh

Anchor Books
New York, 2000
ISBN: 0-385-49532-3



Why should a physicist be interested in codes? The answer is because the latest and greatest challenge in physics involve quantum mechanics. Simon Singh is a very good science writer with interesting anecdotes, and a brisk style with the right level of detail for most readers. The story of codes and ciphers has always been a practical one – at first involving military communications, then business transactions and finally personal freedoms.

One of the oldest known codes is the "Caesar cipher" that moves letters three to the left in the alphabet so that it easy for the reader to decrypt "*Hxuhnd!*" As each encryption algorithm is broken, a more sophisticated one is needed. A latter one uses a "keyword', say *julius caesar*, where duplicated letters are eliminated and then the rest of the alphabet is used to complete the keypad. In this code, the keypad becomes *juliscaert-vwxyzbdfghkmnopq* where letter **A** encrypts to **J**, **E** to **S**, **Q** to **Z**, etc. Without knowing the keyword, this code was thought to be impenetrable and indeed it was for many centuries, until broken by the Arabs in the ninth century using frequency analysis. See if you can read "xrvsrgjasyrkg". The most common letter in English is E which occurs about 13% of the time. Thus using the keyword above, the most common letter (in English) in any (longish) encrypted message would be s and this would quickly identify it as E. The complete code is obtained by following this lead. Unfortunately this technique was not known in the west until it was rediscovered in the sixteenth century. Mary Queen of Scotts used keyword encryption to plot against Queen Elizabeth I from prison, but it was broken by frequency analysis. As a result, she was executed at Fortheringhay Castle, 70 miles north of London, where I write this review.

These kinds of ciphers are "symmetrical" in that decryption is the inverse of encryption and uses the same keyword. This technique was taken further by cyclically rotating the 26 letters of the keypad by one each time a letter was encrypted. There were variants on this – leading to the 'Le Chiffre Indéchriffrable' (The Unbreakable Cipher) of Blaise de Vignere, that was impenetrable for two centuries. This lead to the development of a mechanical version - the 'Enigma' machine - that was used by the Nazis in World War II.

The book tells the familiar story of how the Nazi code was broken at Bletchley Park near Cambridge in England; among the most significant technical advances contributing to the ending of the war (and there were many including radar and the atomic bomb). There was a twice-repeated three letter "day code" at the beginning of each message that gave Alan Turing and others the clue they needed to start to unravel the system.

This was huge team effort, but the next most important advance was made separately by two individuals in a move that made all previous encryption techniques obsolete. Isn't this always the case in science that key advances are made by one or two people, and then it passes onto teams and becomes an engineering problem?

The culmination of symmetric encryption techniques is DES (Data Encryption Standard) and is used in all commercial, banking and internet transactions today. It is fast, reliable and unbreakable unless you know the keyword. The problem is how to get the keyword safely from Alice to Bob. The breakthrough came through Whitfield Diffie, a graduate student at Stanford, who had the idea of asymmetric keys; and Ronald Rivest, a computer scientist at MIT, who proposed using two large prime numbers. It is easy to multiply two prime numbers together like p=17,159 and q=10,247 to give pq=175,828,273, but it is exponentially hard to factor the product pq. This leads to the RSA algorithm with a public key pq that everyone knows and uses to encrypt a message. But the private key p or q must be known to decrypt. Thus no secret message needs to pass between Alice and Bob for secret communication to be initiated. It is quite astonishingly simple and could have been

(Continued on Page 3)

BOOK REVIEW...(Continued from Page 2)

found centuries ago. Today the public/private key system is used for banking, military and diplomatic communication, web transactions and criminal activities where the keyword is passed using the public/private key and then the faster DES method is used for the message itself. This code is available to you via PGP (Pretty Good Privacy) by downloading free programs from the web, and it cannot be broken even by the National Security Agency (NSA) if you use large enough numbers (1024 digits). No number of this size has ever been factorized into primes. To date the largest number factored is pq=15! You can bet the NSA is running scared!

Can the RSA algorithm ever be broken? The history of cryptology suggests it can. This could use DNA or quantum cryptology where things are done in parallel rather than in series. The whole issue is can a large number that is known to be a product of primes be factorized , and in principle the answer is yes and very quickly using a quantum computer. But it is extremely hard to build a workable DNA or quantum computer – it is a practical problem for physics today. If you can do it, you will rule the world!

Reviewed by Michael Thorpe, Foundation Professor of Physics, Chemistry & Biochemistry at ASU.

MNS program...(Continued from Page 1)

program at any other university in the United States, and it stands as an exemplary model of how (university) physics departments can improve high school physics education."

Students in the program come from across the country and nearly all states are or have been represented. Ann Marie Stafford is currently enrolled in the program. She attended the University of Arizona for her bachelor's and master's degree, and enrolled in one of the modeling courses last summer. That course proved so beneficial, that she decided to enroll in the MNS program this summer.

"The modeling method of instruction is proven to increase student conceptual understanding of physics. I have changed my physics instruction to include modeling and find the students do understand the concepts" says Stafford, a chemistry and physics teacher at Marana High School in Tucson who also serves as a 4H leader and science Olympiad coach.

Stafford chose the MNS program to enrich her physics instruction. She finds the blending of graduate level physics content and the attention to physics pedagogy to be the greatest benefit of the program. Through the process of enhancing her own physics instruction, she has developed a long-term aspiration to return the favor .

"I love being a physics and chemistry teacher and will continue to teach for many more years. In the distance future I would love to teach science teachers how to be successful at teaching"

For more information about the MNS program at ASU, please visit http://physics.asu.edu/graduate/mns/overview.

PHYSICS FLASH
WANTS TO HEAR FROM YOU

Please send your comments, questions, and story suggestions to phyflash@asu.edu.

"How I spent my summer vacation"
by ASU Physics

Went to the top of Mount Huangshan in Anhui province, China
- Adam de Graff, biophysics graduate student

Went scuba diving with my sons in Hawaii
- Robert Nemanich, Chair of ASU Physics

Spent time with my daughter and visiting family (here at the Chihuly installation at the Desert Botanical Gardens)
- Peg Stuart, Department Manager