Fun with Cryptography: A Fun Workshop for Sonia Kovalevsky High School Mathematics Day

Tuval S. Foguel and Joan Nunnelley Powell

Honoring the Research and Teaching of Joe Malkevitch

The Sonia Kovalevsky High School Mathematics Day is an annual program of mathematics activities for young women. Grants to help in funding these programs are sponsored by the Association for Women in Mathematics (AWM), the National Security Agency (NSA), and currently Elizabeth City State College. The event is named in honor of Sonia Kovalevsky, who was the first woman to earn a doctorate in mathematics in 1874. The event is designed to encourage high school-aged women to consider pursuing more mathematics and careers in mathematics and the sciences.

Keynote address SK day 2005 AUM

This exciting day at Auburn University Montgomery (AUM) features workshops on mathematics topics outside the normal scope of the high school curriculum, but accessible to and recommended for students enrolled in junior/high school Algebra I and up. We have workshop leaders, some of which are women recruited from off campus, a national speaker who is a woman mathematician, and career panelists from various areas. These professionals share their expertise in math and the panelists share how they entered their careers and the role mathematics played in those careers. These careers have included women teachers at the junior high, high school and college level; college professors in areas like biology, political science, chemistry, psychology, and elementary mathematics education; and professionals from areas including medicine, engineering, geology, computer science, biostatistics, an Air Force Colonel and pilot, and an NSA mathematician. NSA's support of the program included partial or full funding of their employee's travel to the event the years we have obtained an NSA participant.

A unique aspect of this program is that not only is it free to all participants, funding allows us to offer travel reimbursement to those with round trip travel of 50 miles or more and even hotel accommodations for some traveling further. Young women from around the state come to learn new and fun things about mathematics, meet women in math-related careers from Alabama and across the nation, and find out more about careers that use mathematics. Participants interact with mathematics majors and professors from our campus who are on hand to host the event and lead and participate with them in the workshops. Feedback from the five years of this event, 2004 – 2008, has been overwhelmingly positive from students, teachers and parents, citing insightful workshops, great speakers, and interesting career panelists. The great food, a gift for each participant and abundant door prizes didn't seem to hurt either.

Recruiting for the event has focused on mail outs to surrounding counties, with particular emphasis on reaching more widely to include several predominantly black counties in our region. Thus the program addresses participation of two populations underrepresented in mathematics, women and minorities, in our region, particularly African Americans. The overall attendance has ranged from 45 participants to 110 participants, including students, teachers and parents. So many parents, some homeschoolers, have become enthusiastic and full participants in this event. The minority recruiting efforts appear to have worked, with minority student participation peaking in 2007 with 69% of students and 29% of parents and teachers being minority. In 2008, minority student participation was still high at 58% and minority parent/teacher participation peaked at 50%.

The workshops at the AUM Sonia Kovalevsky Day make up a large part of the program. Many of the workshops are "hands on," which is a great way to bring mathematics to life. The workshops are often run in duplicate sessions and, according to the evaluations, three of the more popular ones were "Coding Theory in Your Mailbox," "Sonia Kovalevsky: Who, what, when, why," and "Fun with Cryptography."

Fun with cryptography workshop SK day 2004 AUM

In the workshop titled Fun with Cryptography. We used Power Point for the presentation, since it gave us the ability to add graphics and sounds to the presentation. The presentation took about 25 minutes and the hands on activity at the end took another 25 minutes. The presentation started with some history and explanations of cryptography and Latin squares. Then we introduced the table below, which is a crossed inverse Latin Square. In such a table if a row α is used for encrypting the letters of a plaintext message, then we use the column α ' to decrypt the message.

o	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R
B	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U
C	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X
D	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A
E	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D
F	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G
G	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J
H	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M
I	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P
J	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S
K	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V
L	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y
M	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B
N	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E
O	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H
P	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K
Q	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N
R	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q
S	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T
T	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W
U	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z
V	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C
W	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F
X	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I
Y	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L
Z	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

Where

A' =A, B' = Z, C' = Y, D' = X, E' = W, F' = V, G' = U, H' = T, I' = S, J' = R, K' = Q,

L' = P, M' = O, N' = N, O' =M, P' = L, Q' = K, R' = J, S' = I, T' = H, U' = G, V' = F,

W' = E, X' = D, Y' = C, Z' = B

We gave them an example of encrypting and decrypting

HI

Using C and C' = Y.

o	A	B	C	D	E	F	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	J	S	B	K	T	C	**L**	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R
B	D	M	V	E	N	W	F	**O**	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U
C	**G**	**P**	**Y**	**H**	**Q**	**Z**	**I**	**R**	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X
D	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A
E	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D
F	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G
G	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J
H	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M
I	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P
J	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S
K	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V
L	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y
M	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B
N	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E
O	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H
P	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K
Q	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N
R	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q
S	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T
T	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W
U	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z
V	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C
W	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F
X	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I
Y	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L
Z	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

o	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R
B	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U
C	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X
D	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A
E	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D
F	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G
G	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J
H	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M
I	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P
J	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S
K	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V
L	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y
M	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B
N	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E
O	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H
P	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K
Q	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N
R	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q
S	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T
T	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W
U	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z
V	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C
W	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F
X	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I
Y	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L
Z	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

So

HI→RA

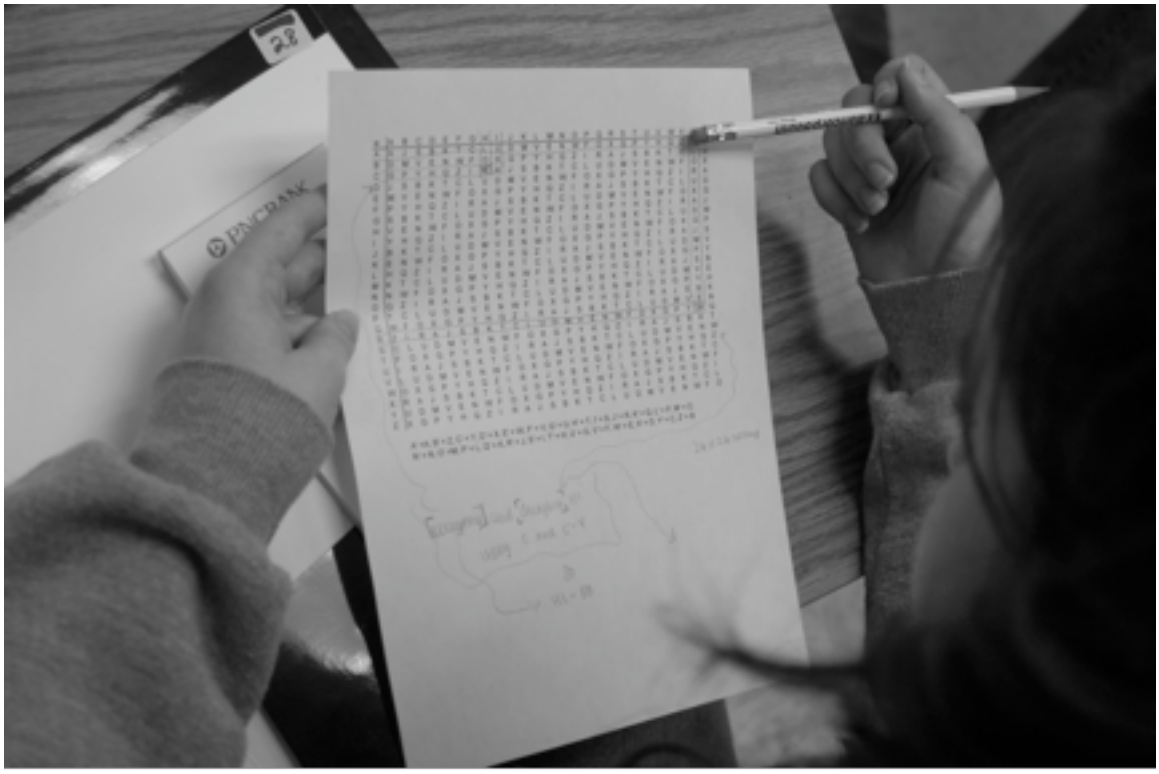
Afterwards we used the C' = Y column to decrypt RA→HI.

Next we challenged the students to decrypt the following lyrics,

MXF TONNYJ PNNI ZQ SBAQXQF

VDAAL HN OZHN SZ JNN HL PXQ

JXQFXQF JZQFJ DMZBS SON JZBSOYDQE



Decrypting RA

and give the title of this song, given that we used the B row to encrypt it. The student that was first to give the title got to click on a link in the presentation that played the song (the song is *Sweet Home Alabama*).

Lyrics :

BIG WHEELS KEEP ON TURNING

CARRY ME HOME TO SEE MY KIN

SINGING SONGS ABOUT THE SOUTHLAND**.**

Team work in decrypting the lyrics

In the end of the presentation we had students choose a letter and use it to encrypt the name of a favorite movie and give the letter and the encrypted message to the person sitting across from them to decrypt. We walked around to help them encrypt and decrypt. We were happy to see that they also got help from fellow students. The workshop lasted 50 minutes; the highlight was the hands on experience.

AUM Sonia Kovalevsky Day provides a much needed outreach to high school students and a substantial enrichment to the education that these young women receive. The number of young women, particularly minorities, enrolling in the mathematics major is very small locally and nation wide. We believe that Sonia Kovalevsky Day can encourage more female students to seriously consider mathematics and to recognize that there are a wealth of interesting careers open to them in math and related fields.

Tuval S. Foguel and Joan Nunnelley Powell
Auburn University Montgomery
Department of Mathematics
P.O. Box 244023
Montgomery, AL 36124-4023, USA
email:{tfoguel, jpowell}@aum.edu