



# VIRGINIA MOUNTAIN SECTION NEWSLETTER

IEEE Region 3, Council 09, Section 65

September 2008

Thursday, September 18, Holiday Inn Hotel Roanoke Airport

## Chocolate Key Cryptography – A Delicious Way to Send Secret Messages

presented by

**Dr. Ezra Brown**

Alumni Distinguished Professor of Mathematics  
Department of Mathematics, Virginia Tech

### Abstract

The art and science of secure communication is called cryptography. To send someone a secret message, you need two things:

1. a way to scramble the message ("the cryptosystem"), and
2. a piece of information that tells the sender and the receiver just how the scrambling is done ("the key").

Keeping the key in the right hands and out of the wrong hands is a major problem for cryptographers, and public key cryptography is a solution to this problem that is at work on every computer and in every network in the world.

This talk is about Chocolate Key Cryptography, which is a way to describe a certain public key cryptosystem that is easy to learn, fun, interactive, and delicious.



### Biographical Sketch

Ezra (Bud) Brown grew up in New Orleans, has degrees from Rice and LSU, and has been at Virginia Tech since 1969, where he is currently Alumni Distinguished Professor of Mathematics.

Although most of his research has been in number theory and combinatorics, he once wrote a paper with a sociologist. During the

summers, he works on problems of cryptography and cryptanalysis with an unnamed government agency. He has been honored with some teaching and writing awards. He enjoys singing in operas, playing jazz piano, gardening, and talking about his granddaughter Phoebe Rose. He occasionally bakes biscuits for his students.

**Date:** Thursday, September 18, 2008

**Social:** 6:30 PM

**Dinner:** 7:00 PM

**Talk:** 8:00 PM

**Cost:**

Members & Guests \$20.00

Students \$10.00

**Reserve by 5 PM Monday  
September 15, 2008**

**Dr. Wilbur Dale (540) 464-7547**

[mail to:dalewn@vmi.edu](mailto:dalewn@vmi.edu)

Please specify the number of attendees.

## Directions to Holiday Inn Hotel Roanoke Airport

2727 Ferndale Drive NW

I-581, Exit 3  
Hershberger Rd West  
1st Rt. onto Ordway Drive,  
¼ mile, Rt. into parking lot.

---

### Student Chapter Websites

VMI: <http://ieee-vmi.org>

VT: <http://www.ieee.vt.edu>

---

## Editor's Note

Greetings! I've taken over the task of getting the newsletter out to the VMS from Dr. Ira Jacobs. I know I speak for the section when I express a deep-felt gratitude to Dr. Jacobs for his work in producing a well-structured and timely newsletter as well as managing its distribution via the listserv. I hope I am able to perform the job at the same level of excellence.

My plan is to continue to deliver the newsletters two weeks in advance of the meetings. If you

have an announcement, article, or opinion to be included in the newsletter, please get it to me via email at least three weeks in advance of the meetings.

At the bottom of the page, I've added a new feature, "Meanwhile, Back at the Lab..." Hopefully it's good for a giggle and won't stimulate your gag reflex too often.

We'll see you at the meeting.

Dave Livingston

---

## Election Season

The organization Scientists and Engineers for America (SEA) has teamed with other science and technology organizations, including IEEE USA, to get the views on science and technology issues of candidates for national offices. This information is available at:

<http://sharp.sefora.org/>

---

### VMS Officers

Chairman: **Wilbur Dale**  
[mail to:dalewn@vmi.edu](mailto:mail.to:dalewn@vmi.edu) 464-7547

Vice Chairman: **Chris Bonadeo**  
[cbonadeo@verizon.net](mailto:cbonadeo@verizon.net)

Sec./Treasurer: **F. Gail Gray**  
[fggray@vt.edu](mailto:fggray@vt.edu)

### VMS EXECUTIVE COMMITTEE

David Geer [dgeer@ieee.org](mailto:dgeer@ieee.org)

Robert Hendricks  
[hendrwr@vt.edu](mailto:hendrwr@vt.edu)

Ira Jacobs [ijacobs@vt.edu](mailto:ijacobs@vt.edu)

Edward Tuttle  
[tuttleone@earthlink.net](mailto:tuttleone@earthlink.net)

Junior Past Chairman: Jan Helge Bohn  
[bohn@ieee.org](mailto:bohn@ieee.org)

### VMS CHAPTER CHAIRS

Computer, Control Systems, & Industrial Electronics:  
Lynn Abbott [abbott@vt.edu](mailto:abbott@vt.edu)

### NEWSLETTER

Editor: **Dave Livingston**  
[d.livingston@ieee.org](mailto:d.livingston@ieee.org)

540-464-7545

Contact the newsletter editor to be added to the VMS listserv.

### WEBSITE

<http://www.ewh.ieee.org/r3/virginia-mountain>

Webmaster: **Chris Bonadeo**  
[cbonadeo@verizon.net](mailto:cbonadeo@verizon.net)

Meanwhile, Back at the Lab...

Livingston

