For a calendar of technical society meetings in the Mid-Hudson Valley go to:
http://pok.acm.org/calendar.html and/or to MHVLUG's calendar at https://mhvlug.org/calendar

Poughkeepsie Chapter of the Association For Computing Machinery

```
  aaa          ccccccc       mmmmmm   mmmmmm
 a   a        cc     cc     mm  mm    mm  mm
aa    aa      cc       c    mm  mm mm   mm
aaaaaaaaa     cc            mm   mmm    mm
aa     aa      cc      c     mm    m     mm
aa     aa       cc    cc     mm          mm
aa     aa        ccccccc     mm          mm
```

MEETING NOTICE

Free and open to the public

Topic: **Matrix Methods for Private Key Cryptography**

Speaker: **Frank Rubin**

When: **Monday, April 23rd, 2018, 7:30 pm**

Where: **Marist College, Hancock Center, Room 2023**

Directions: **Building 14 on the map at http://www.marist.edu/about/map.html**

Parking: Please park at black dot #10 on http://www.marist.edu/about/map.html (the lot North of the Hancock Center #14) or in the lot on the South-East corner of Route 9 & Fulton St. (S/E of the former Main Entrance).

About the Topic: Private Key cryptography has significant advantages over both Secret Key cryptography and Public Key cryptography. Secret Key cryptography requires that both parties have the same secret key, hence there needs to be a mechanism for distributing the secret keys. Public Key cryptography requires that each party knows the public key of the other party, hence there needs to be a mechanism for distributing the public keys.

In Private Key cryptography each party uses a private key unknown to the other party. There is no need to ever distribute these keys. Keys may be generated at will and discarded after one use.

Private Key cryptography can be achieved using the Three-Pass Protocol and matrix multiplication. Encryption, decryption and key-generation are as fast and simple as matrix multiplication, and there is no need to use numbers any larger than 8 bits. The matrix multiplication can also be used to establish secure keys for conventional cryptography, such as AES.

About the Speaker: Frank Rubin has an M.S. in Mathematics and a Ph.D. in Computer Science. He worked as a programmer for IBM in Design Automation from 1964 to 1991. He originated many of the algorithms still used for laying out and wiring chips and circuit boards.

He has been involved in cryptography since high school. He has been an editor of the hobbyist publication The Cryptogram, and the professional journal Cryptologia. He teaches a course on cryptography at Marist CLS (Continuing Life Studies). He is also the author or inventor of thousands of puzzles, some of which can be found on his websites.

Cost: **Our meeting is Free and open to the public**

Dinner: **6:00 pm, Palace Diner, 845.473.1576**
Map and menu: www.thepalacediner.com
All are welcome to join us for dinner.

We thank Marist College for hosting the chapter's meetings.

P - L - E - A - S - E P - O - S – T

This page is available on the web at http://pok.acm.org.