DACS.doc

A Computer & Technology Newsletter

February 2017 Volume 28, Issue 2 $2.00

Next Event:
Tuesday, February 7,
7:30 PM

Online Marketing: Five Mistakes to Avoid on Your Website

Directors' Notes

Danbury Area Computer Society (DACS)

Board Meeting Minutes
Wednesday, January 4, 2017

The meeting was called to order at 7:07pm by the DACS President, Dave Green.

In attendance were board members Richard Corzo, Bert Goff (Secretary & Treasurer), Dave Green (President), Jim Scheef, and Andy Woodruff. Dick Gingras was not present. The minutes were taken by Richard Teasdale.

(Names in italics denote responsibilities for actions.)

• The Minutes of the 12/7/2016 Board Meeting were accepted.

Reports

• The Treasurer's report for December was discussed. Bert reported that dues receipts for the year 2016 were significantly less than in 2015, however expenses were also less than the prior year, making for a net loss in 2016 of under $200. (Bert noted that two December dues receipts were accidentally omitted and so an amended report will be issued.) The initial response to the Resource Center Capital Campaign has been encouraging.

• Membership committee:

o Jim reported 90 paid-up members (including 1 new), and 8 in-grace, for a total of 98. (The Membership report will also be amended.)

o 31 people attended the January 3 General Meeting, 10 of whom were visitors, including several first-time visitors.

• Press Coverage:

o Dave reported that press releases for the January general meeting were sent out on December 22. One recipient (Hamlet Hub) acknowledged the release.

• Website:

o Richard reported that another instance of compromised files was detected by Wordfence. The compromised files were restored by Annette.

o Jim reported that he will install a new release of CiviCRM in the near future.

o Access to the DACS website is still blocked from WCSU's campus network by McAfee Site Advisor, due to the recent hacking. Two requests for review have been filed with McAfee by WCSU, without result.

Old Business

• Programs:

o David Fischer will speak at the February general meeting on the subject of "5 Mistakes to Avoid on Your Website". Richard will write the Preview, and Andy will write the Review.

o *Dave* will speak to the manager of Best Buy about a possible speaker for the topic of Wearable Devices.

o Two potential topics were suggested by Steve Harkness at the January general meeting: (1) drones, and (2) a new hackerspace planned for New Milford. It was agreed that both of these would be good general meeting topics, if suitable speakers can be found. Bert will follow up on either or both.

• Renovation of the Resource Center (RC):

o It was agreed that it would be desirable to approach businesses as well as individuals for donations. Jim and Bert were appointed to a committee for that purpose.

o Andy reported on the status of his dealings with Meadow Ridge for acquiring a donation of used carpet.

• Jim announced his retirement from the DACS Board of Directors. He pointed out the need for a second person to have in-depth knowledge of CiviCRM.

• Potential new directors were discussed. Andy pointed out that people who live far away can attend meetings via Skype, and therefore should not be discounted for that reason alone.

• Slack: Experience with Slack was discussed further. Richard reported that the Linux workshop is not interested in using it.

• Richard Teasdale has volunteered to continue Jim's work on a survey of the membership to determine the level of interest in a NAS workshop, using the

IN THIS ISSUE

Membership Information

dacs.doc, ISSN 1084-6573, is published monthly by the Danbury Area Computer Society, 65 Legion Rd, New Milford, CT 06776. Annual subscription rates: $60 to regular members, $40 electronic access (included in dues).

Postmaster

Send address changes to Danbury Area Computer Society, Inc., 4 Gregory Street, Danbury, CT 06810-4430.

Editorial Committee

Managing Editor: Richard Teasdale
Production Editor: Allan Ostergren

Contributors

Charles Bovaird Richard Corzo
Drew Kwashnak Lisa Leifels
Dave Mawdsley Bruce Preston
Jim Scheef Annette van Ommeren
Andy Woodruff

DACS, its officers and directors assume no liability for damages arising out of the publication or non-publication of any article, advertisement, or other item in this newsletter.

The editors welcome submissions from DACS members. Contact Richard Teasdale (*dacseditor*@dacs.org). Advertisers, contact Charles Bovaird at (203) 792-7881 *(aam@mags.net)*

Copyright

Dick Gingras APCUG Liaison
rgingras@dacs.org

Officers

DACS GENERAL NUMBER: (203) 744-9198
PRESIDENT: David Green *dacsprez@dacs.org*
VICE PRESIDENT PROGRAMS: *vpprograms@dacs.org*
SECRETARY: Bert Goff • **TREASURER:** Bert Goff

Directors

dacsboard@dacs.org

Richard Corzo	(203) 797-1518	*rcorzo@dacs.org*
Richard Gingras	(203) 426-1780	*rgingras@dacs.org*
Bert Goff	(860) 355-8895	*bgoff@dacs.org*
David Green	(203) 797-8682	*dgreen@dacs.org*
Andy Woodruff	(203) 744-9588	*awoodruff@dacs.org*

Committees

NEWSLETTER: Richard Teasdale: *dacseditor@dacs.org*,
PROGRAM: *vpprograms@dacs.org*
WEB MASTERS: Richard Corzo (*rcorzo@dacs.org*), (203) 797-1518
Annette van Ommeren (*avanommeren@dacs.org*), (914) 232-0149
PRESS RELEASES: Dave Green (*dgreen@dacs.org*)
APCUG LIAISON: Dick Gingras (*rgingras@dacs.org*)
MEMBERSHIP COORDINATOR: Jim Scheef *(membership@dacs.org)*
RESOURCE CENTER: (203) 748-4330 • **WEB SITE:** *http://www.dacs.org*

HelpLine

Our former telephone HelpLine has been replaced by our web-based DACS Community Forum at *http://forum.dacs.org*. We have topic-specific forums where DACS members can post questions. Questions may be answered by Workshop leaders or other DACS members. If none of the categories fit your question, just post it to the Ask DACS forum.

Topic	**Forum**
Linux	Linux Workshop
Desktop publishing and website design	Web Site Design Workshop
Mac and iPhone/iPad/iPod touch	Apple Workshop
Online/small business	Online Business
Single board computers	Single Board Computers
Smartphones & Tablets	Mobile Devices Workshop
Social media	Social Media
Video capture/processing	Video
Windows	Windows Workshop

SurveyMonkey account created by Jim. Other options for eliciting feedback from the membership were discussed. The desirability of a survey about a single topic, i.e. NAS, was questioned. *Richard T* will initiate a discussion with board members via Slack to determine if and how to proceed.

New Business

- Snacks for general meetings:
  - o *Richard* (drinks) and *Lisa* (snacks) will make the arrangements in February.
  - o It was agreed that non-board members should have the opportunity to provide snacks.
- Parking options at the Resource Center were discussed.

The meeting was adjourned at 8:40 pm

—*Richard Teasdale*

Uncle DACS Wants YOU!

We rely on volunteers for all our activities. Current positions include:

Vice President: Help the president and eventually become new president.
Social Media: Help DACS post interesting technical content
Painters: Help with the renovation of our resource center.
Workshop Leaders: Organize a group, or join an existing one.

January Meeting Review

Jay Ferron on Microsoft HoloLens

By Angel Cortez

HOLOLENS, Microsoft's augmented reality (AR) smart glass, provides a glimpse into the future of computing. HoloLens is the first cordless, self-contained augmented reality computer running on Windows 10. The HoloLens is similar to Google Glass, which uses AR technology as well.

Microsoft HoloLens is made up of specialized components which, assembled, enable Holographic Computing. The internal HPU of the HoloLens (Holographic Processing Unit) allows for processing of large amounts of data per second (terabytes of data [1]). All these components come together to allow for a freer and more interactive experience with Holograms.

So what is the difference between augmented and virtual reality (AR vs VR)? Virtual reality immerses the user by making them feel like they are experiencing the simulated reality firsthand, by stimulating their vision and hearing. An example of a virtual reality device would be Facebook's Oculus. Augmented reality differs because it adds an extra dimension over virtual reality by showing the real world around the user with a Hologram overlaid. AR can also totally immerse the user, just like VR, by simply displaying pixels everywhere with transparency to the real world. In the virtual world, users are advised to stay stationary to avoid harm from the physical world they cannot see.

Unlike its competitors, HoloLens is not just a visor connected to a computer; HoloLens is a standalone computer. HoloLens contains an Intel Airmont (14nm) processor with four logical processors and is 64-bit capable, a 16,500 mWh battery, a GPU with 114 MB of memory, 918 MB of RAM, and a first of its kind HPU. With 18 sensors built-in that help flood the 14 nm Intel Airmont processor with terabytes of information to process, it is impressive, to say the least.

One of these sensors includes a depth camera that has a field of vision which spans 120 by 120 degrees. The depth of field allows for the HoloLens to sense what your hands are doing even when they are out of direct field of view. Another sensor tracks where the wearer is looking, so that it may adjust the Holograms accordingly. Yet another sensor detects the wearer's movements. These sensors help track the hands, so the hands can act as an input system. In addition, the user can interact with physical or virtual objects, which are detected by the camera sensor. These sensors also allow for the detection of pre-programmed gestures, which enables the tracking of user movements.

Microsoft HoloLens has a User Interface so that it can process voice, gaze, and gestures as input commands. The processor then takes these modes of input and computes accordingly.

Projection of the Holograms is done using the HUD (head-up display) method. This is done using two individual Nano projectors located at each side of the head unit and the semitransparent visor, which then reflect the image as light on the user's eyes. Additionally, HoloLens has two displays. These two displays are transparent so that the wearer can see the real world behind the virtual object. To create a projected HoloLens image, light particles bounce around millions of times in the so called light engine of the device.

With the development of Windows 10, Microsoft revealed that it is the first platform to support Holographic Computing, with APIs that enable gaze, gesture, voice, and environmental understanding on an untethered device.

The Microsoft HoloLens is packed with Sci-fi like features. HoloLens brings high-definition holograms to life in the world around you, where they integrate with your physical places, spaces, and things. Your digital content and creations will be more immersive when they come to life in the surrounding world, and you can interact with them via HoloLens.

Microsoft HoloLens is more than a simple heads-up display, and its transparency means you bring the digital world into the real world around you. High-definition holograms integrated with the physical world will unlock new ways to create, communicate, work, and play.

HoloLens creates all-new ways to teach and learn. Most us would agree it's easier to show than to tell, but why not do both? With Microsoft HoloLens, friends and colleagues can help you with difficult tasks using HoloNotes in Skype. It's almost like having your help be right there in the room with you.

HoloLens will revolutionize how you design and develop the future. As holograms, your digital content will be as real as physical objects in the room. For the first time, holograms can become practical tools of daily life. Imagine, instead of going into a store to try on a new dress you could have the dress appear right in front of you. Or imagine, designing home renovations without every needing to leave the comfort of your home.

HoloLens will change the way we travel. With Microsoft HoloLens we will be able to explore the rainforests of the Amazon, the surface of Mars, or the deepest depths of our planets oceans without ever having to risk bodily harm.

With the power of HoloLens, we will be able to visualize what our designs will look like in the physical world, whether it's a new pool for your home, a toy for your children, or a new creation for work.

Some of the advantages of Microsoft HoloLens include: ease of use and wear, sensitivity and responsiveness to the prescience of people, and practical applications from battlefield to the drawing board. The Microsoft HoloLens is more than useful technology for designing and facilitating future innovation.

Many people attempt to draw comparisons between the Microsoft HoloLens and the Google Glass, but there are apparent and significant differences between the two products. For example, Google Glass was designed to perform similar functions to those of a modern Smartphone. Like a Smartphone it supports Apps, takes photos and video. In the end, Google Glass is an expensive version of a handheld device. In addition, Google Glass supports virtual reality where users disconnect from the real world, but HoloLens users see and immerse themselves in both the digital and physical world in front of them. HoloLens users can walk around and talk to others without worrying about bumping into walls or any eye strain.

However, there are some clear drawbacks to the Microsoft HoloLens. First, it can easily be damaged or broken due to all the sensitive sensors (18 sensors). Second, using the device while driving is not recommended (may lead to car accidents). Third, there are some privacy concerns due to the onboard camera of the HoloLens. Finally, the price of the device ($3,000 for the developer Edition and $5,000 for the Commercial Suite).

All in all, the Microsoft HoloLens brings a whole new realm of possibilities to both the digital world and the physical world. The era of holographic computing is here to stay. Microsoft is helping shift the digital spectacle from your pocket to your eyes.

Sources

1.http://news.microsoft.com/speeches/satya-nadella-terry-myerson-joe-belfiore-and-phil-spencer-windows-10-briefing/

February Meeting Preview

Online Marketing

By Richard Corzo

Date: Tuesday, February 7, 7:30 p.m.
Location: Danbury Hospital Auditorium
Presenter: David Fischer

AT OUR FEBRUARY MEETING independent consultant David Fischer will give his presentation "Online Marketing - Strategies and Tools for an Effective Online Presence." Leveraging what he learned in the corporate world, he left to found Solutions for Growth LLC, which helps small businesses, non-profits, and professional practices to market themselves.

Attend this information-packed seminar and learn the strategies behind having an online presence, the many available channels and specifics of "how-to."

This practical seminar will provide a concise and comprehensive overview of online marketing best practices and easily avoidable mistakes.

You'll discover which online tools are a "must," which are best for customer acquisition and which are ideal for development of customer loyalty and repeat business.

The presentation will cover:

- Websites
- Online Marketing
- Search Engine Optimization
- Google AdWords
- Social Media
- Email Marketing

You'll have plenty of time to ask questions, share experiences and network with peers. You'll leave with real-world insights and knowledge that you can put to work immediately to help your business succeed.

David Fischer founded Solutions for Growth to help small businesses increase sales and grow. He brings over 25 years of marketing experience across a range of industries. His corporate experience allowed him to identify the marketing techniques that can be successfully applied to non-profits, small businesses and professional practices.

Solutions for Growth counts clients locally and in nearly 40 states.

Solutions for Growth helps increase sales through proven, practical and achievable marketing tools that have allowed businesses to flourish. Through valuable and smart solutions, David shares marketing knowledge and experience that enable his clients to grow.

Read the Blog on dacs.org

For the past several months, Jim Scheef has been posting to a blog on the club's website. You can read these posts at *https://dacs.org/category/news/*. We are looking for a few volunteers to help contribute to this blog. To qualify, you must be a member in good standing and be willing to post regularly, meaning one or more posts weekly. You will receive training in how to enter and format the blog posts (a little HTML can be helpful).

Content must be related to the club's mission of learning and sharing information about computers and how we use them. There is tons of interesting and valuable information to share and one person cannot find and post it all.

If you're interested, email the webmasters.

Workshops

Workshop NOTES: February 2017

Apple. Focuses on all aspects of the Mac and iPhone operating systems.

Contact: Richard Corzo (*applesig@dacs.org*).
Meets 2nd Tuesday, 7 p.m. at DACS Resource Center.
Next Meeting: Feb 14

Jobs. Networking and jobs search

Contact: Charles Bovaird, 203-792-7881 (*aam@ mags.net*). Go to DACS Community Forum (*http:// forum.dacs.org for job listings*.

Linux. Helps in installing and maintaining the Linux operating system. Also of interest to Apple owners using OS X.
Contact: Dave Mawdsley, *linuxsig@dacs.org*

Meets 3rd Wednesday, 7:30 p.m. at the DACS Resource Center.
Next Meeting: Feb 15

PC Maintenance. Review of PC hardware and OpSys maintenance and use.
Contact: Charles Bovaird, 203-792-7881 (*aam@mags.net*).
Go to DACS Community Forum (*http://forum.dacs.org*).

Online Business Workshop. Informal member gathering sharing ideas on creating an online source of income.
Contact: Steve Harkness (*onlinebizsig@dacs.org*)
Meets second Monday in Brookfield, or by Webinar.
Next Meeting: Check *dacs.org*.

Single Board Computers Workshop. Explores small cheap computers like Raspberry Pi, Arduino, Netduino, Beaglebone, and more. Meets at 7:30 p.m on the 3rd Thursday at the DACS Resource Center.
Contact: Jim Scheef (860-355-0034)
Next Meeting: Feb 16

Video Production. The Video Workshop explores all aspects of video capture and production, including both inexpensive and professional choices for cameras and editing software.

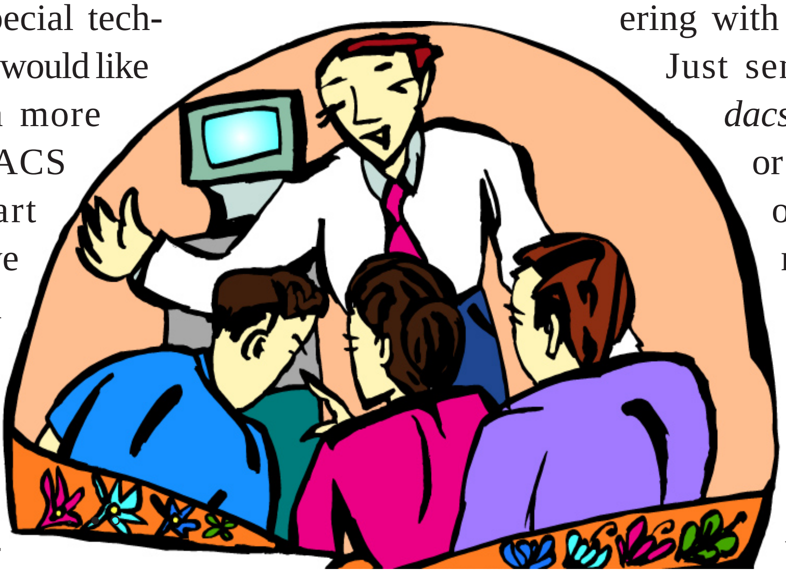
Meets on the 4th Thursday of certain months, typically at 7:00 pm at the Resource Center. Check the Calendar for details.
Contact: Andy Woodruff (awoodruff@dacs.org)
Next meeting: Check dacs.org

Web Development/Design This workshop is on temporary hiatus. Would you like to take on the role of workshop leader? It's a great way to share information, learn new techniques, promote your business, and interact with like-minded people. Extensive web knowledge is not required, but a willingness to open a topic for discussion and enjoy the contributions and feedback from the attendees. Contact Annette for more information. Next meeting: Tentative start up again in April 2017.

Contact: Annette Van Ommeren (avanommeren@dacs.org)
Next meeting: Check dacs.org

Let's join heads!

Do you have a special technology interest you would like to share or learn more about? Join a DACS workshop or start one. You don't have to be a nerd or a guru—just have a curiosity for what's out there and an interest in sharing or discovering with others like you. Just send an e-mail to *dacsprez@ dacs.org,* or talk to one of our officers at the next meeting, and say something like "I want to start a workshop!" or "Wouldn't it be nice if we had a workshop on . . .?"



February 2017

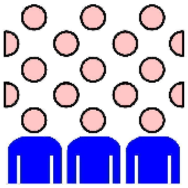
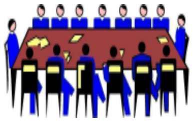
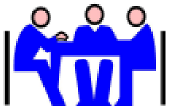
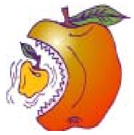
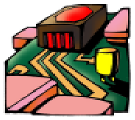
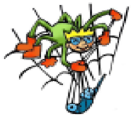
Danbury Area Computer Society

Jan 2017

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Mar 2017

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3	4
5	6	7  **General Meeting** 7:30 PM	8  **Board of Directors** 7:00 PM	9  **Membership Committee** 7:00 PM Jim Scheef 860-355-0034	10	11
12 	13	14  **Apple** 7:00 PM Richard Corzo *applesig@dacs.org*	15 **Linux** 7:30 PM Dave Mawdsley *linuxsig@dacs.org*	16  **Single Board Computers Workshop** Jim Scheef 860-355-0034	17	18 **DACS.DOC Deadline**
19	20	21  **Web Development and Design** Annette van Ommeren 7:00 - 9:00 PM *avanommeren@dacs.org* **On Hiatus**	22	23	24	25
26	27	28				

Encryption Technology

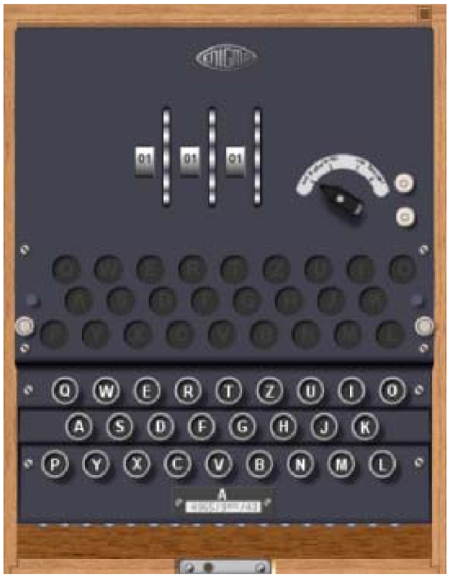
Crypto Simulation

By Dick Maybach

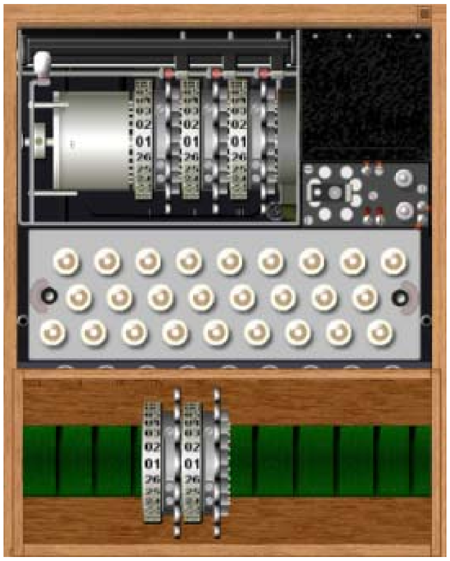
MOST CHILDREN ARE fascinated by encryption; certainly, I was. I still remember having to ask my dad for help in learning to use my Captain Midnight Code-O-Graph, which encoded messages by replacing letters with numbers. Given the popularity of documentaries and movies about the British efforts to decode German Enigma messages during World War II, many adults, including me, retain this interest. Understanding modern encryption requires a sophisticated math background, and slogging through a description can be truly tedious. The simple mechanical devices used during World War II are more approachable and have much historical interest. A fascinating way to learn about them is to run simulations on your PC. You can follow the same procedures and tap the same keys that WWII German and American soldiers did, and by doing so obtain a much better understanding of the processes than by watching a movie or reading a book.

The Enigma is probably the most famous cryptographic device ever. Not only was it effective at the time, but it also significantly influenced World War II. Thousands died as a result of the successes and failures of attempts to decrypt messages encoded by it. The best way to learn about Enigma is to use one. While actual units are available, they are expensive. Instead, you can download an excellent free simulator from http://users.telenet.be/d.rijmenants/index.htm, a site in Belgium maintained by Dirk Rijmenants. Here you can find simulators for several historic crypto machines, instructions for using them, and their histories. These are Windows programs, but OS X users can run them using Crossover and Linux users with Wine. Like all similar devices of that era, the Enigma is a mechanical device, which used a set of disks to scramble the connections between the 26 letter keys of a keyboard and 26 lamps. At least one disk moved at each key press, so that pressing the same key twice produced two different output letters. A battery was needed only to illuminate the lamps. Mechanical connections between the keys and the rotors moved the latter.

Screen 1 shows the keyboard, the (unlit) output indicator lamps, the edges of the three rotors, the power switch, and the terminals for external power. There are some complications, but basically the operator selected three (of the five available) rotors and inserted them in the correct order. Then he rotated them to a given starting position and began typing. The indicator lamps remained lit only while the key was pressed, and a second operator was needed to record the output.



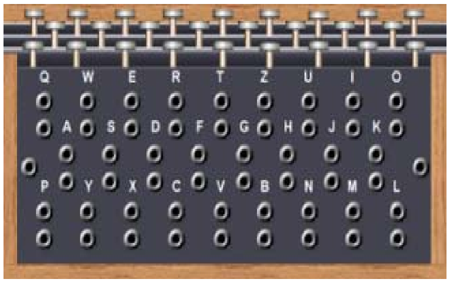
Screen 1. Enigma Panel.



Screen 2. Enigma Interior.

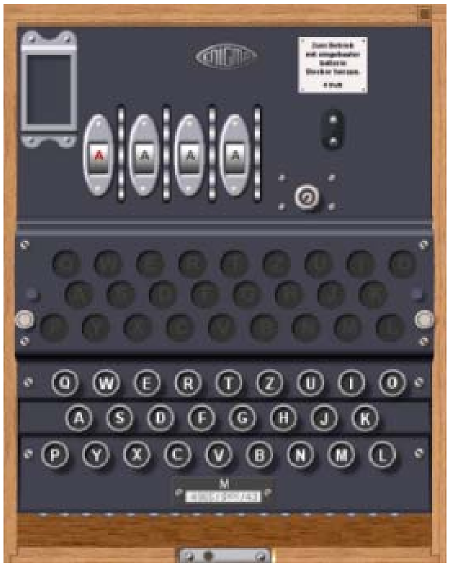
Screen 2 shows the same machine with its cover lifted. The three installed rotors are at the top and the two unused ones in a rack at the bottom. The unused rotors were stored in a separate box, which the simulator shows sitting on top of the keyboard mechanism. The empty space to the right of the rotors is for the battery.

A further complication was provided by a plugboard, Screen 3, that scrambled the connections between the keyboard and rotors. The simulator also includes this feature to allow setting the Enigma up exactly as it was used.

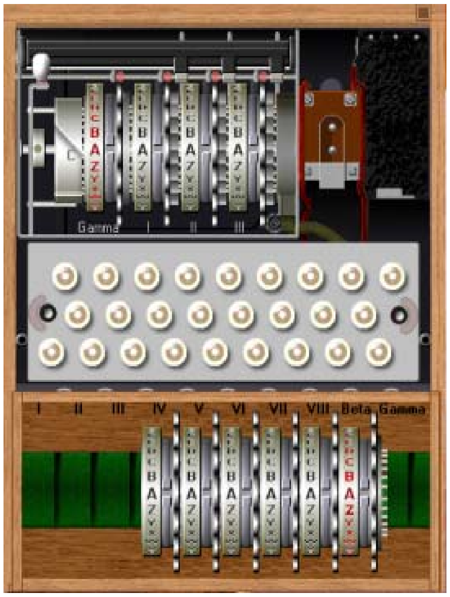


Screen 3. Enigma Plugboard

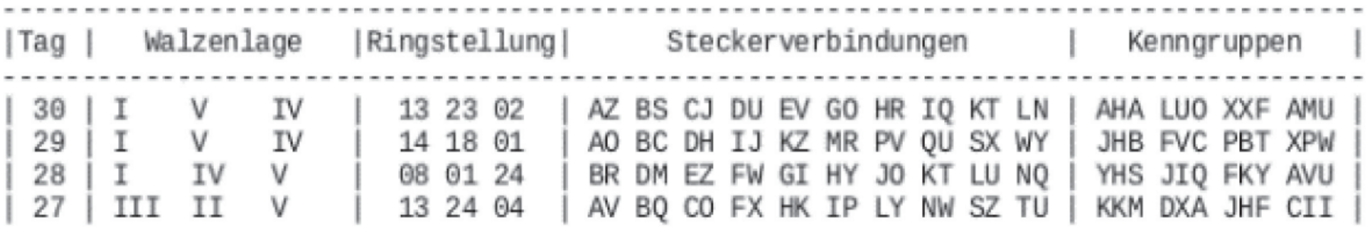
.Enigma was really a family of devices. Screen 4 shows a model used by the German navy. It had no internal battery, and used a plug instead of screw terminals for power.



Screen 4. Enigma Model Used by the German Navy. With four rotors instead of three, this was more secure.



Screen 5. Interior of the Navy Enigma.



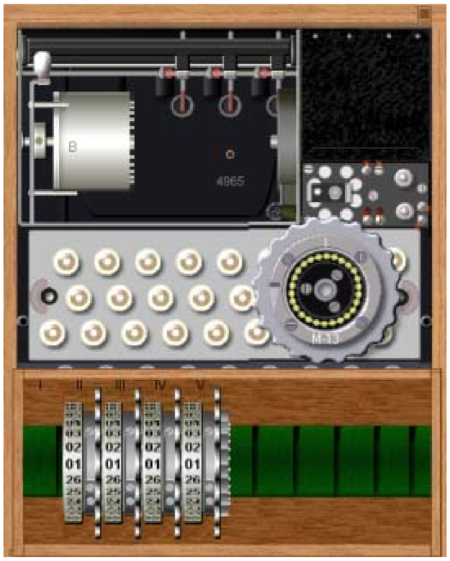
```
--------------------------------------------------------------------------------------------
|Tag |   Walzenlage   |Ringstellung|       Steckerverbindungen       |   Kenngruppen   |
--------------------------------------------------------------------------------------------
| 30 | I    V    IV   |  13 23 02  | AZ BS CJ DU EV GO HR IQ KT LN | AHA LUO XXF AMU |
| 29 | I    V    IV   |  14 18 01  | AO BC DH IJ KZ MR PV QU SX WY | JHB FVC PBT XPW |
| 28 | I    IV   V    |  08 01 24  | BR DM EZ FW GI HY JO KT LU NQ | YHS JIQ FKY AVU |
| 27 | III  II   V    |  13 24 04  | AV BQ CO FX HK IP LY NW SZ TU | KKM DXA JHF CII |
```

Screen 6. Enigma Codebook Sample.

As shown in Screen 5, navy operators had more rotors to choose from, although only the Beta and Gamma units (those with red letters) could be used in the fourth slot.

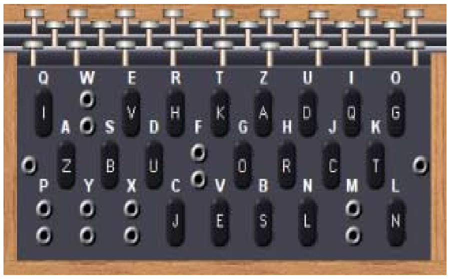
To see how the Enigma was used, let's work through an example. The first step is to consult a codebook, Screen 6, for the machine settings of the day. There was a separate page for each month, with a line for each day (Tag in German). Using the sample, we see that for the 30th of this month we are to use rotors I, V, and VI, with offsets of 13, 23, and 02, respectively. The offset is how much the rotor should be rotated with respect to its outer numbered shell. (If you download the Enigma simulator, be sure also to get the Enigma Code Book Tool, which generated this example.)

Screen 7 shows a rotor I removed from the case (by right-clicking on it) and offset by 13 (with repeated clicks on the upper part of the rotor). We'll put it back in the case by right-clicking on the empty position and then set rotors V and IV similarly.



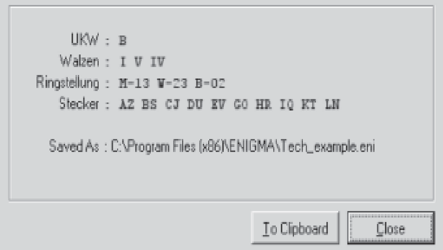
Screen 7. Enigma Being Configured.

The Steckerverbindungen column shows the plugboard connections. It tells us to swap A with Z, B with S, and so on. On the simulator, click on the lower edge of the keyboard to show the panel, Screen 8. (Note that the jacks are arranged like a QWERTY keyboard.) On the actual machine, A and Z would be swapped by connecting the A and the Z jacks with a cord; on the simulator, just click first on A then on Z. The screen-shot shows the panel set-up complete. Note that the A-jack pair is covered with a black shape labeled Z and that the Z pair has a shape labeled A. This is true for all 10 swaps called for in the codebook.



Screen 8. Configured Plugboard.

The simulator provides a check of the setup -- shown in Screen 9. It shows we've used a B reflector (the cylinder to the left of the rotors and the only one available for this model), the arrangement of the rotors, their offsets, and the plug settings. It also allows us to save the settings for later use.



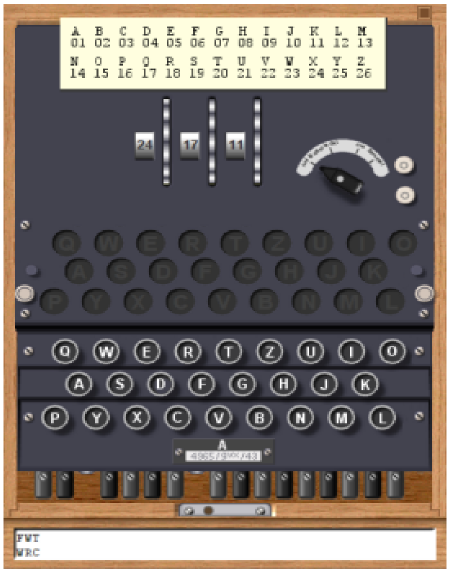
UKW : B
Walzen : I V IV
Ringstellung : M-13 W-23 B-02
Stecker : AZ BS CJ DU EV GO HR IQ KT LN

Saved As : C:\Program Files (x86)\ENIGMA\Tech_example.eni

Screen 9. Enigma Simulator Check Screen.

While the settings from the codebook were typically used for one day, each message has its own key. To send a message, the sender first chose two three-letter keys, for example XPH and FWT and used the first to encode the second. In effect, XPH is the key for a three-letter message. For Enigma, a key is the initial setting of the three rotors. Although the keys are specified as letters, the rotors are labeled by numbers, so there was a table attached to Enigma relating the two. The simulator can display this, as shown in Screen 10. The window at the bottom shows the input and output, where we see that FWT has been encoded as WRC. The sender then composes a message header, such as the one shown below.

F7Z DE WN 1340 = 38 = XPH WRC =



A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

FWT
WRC

Screen 10. Enigma Simulator in Use.

The sending station is WN; the receiver is F7Z, the time is 1340, and there are 38 characters in the message. Only if the receiving Enigma is set up exactly the same as the transmitting one, will it produce the correct message key, and because only three characters are coded, breaking it is nearly impossible. (Although some lazy operators reused keys, and the British made use of this.) The transmitter now resets the rotors to FWT and encodes the message, in this case, "Preserve wildlife. Pickle a squirrel." Note that there are no number, punctuation, or space keys. Words will be run together, and we'll use X to end sentences, as did the Germans. If there were digits, we would have to spell them. A complete encrypted message appears below. As is customary the letters shown as five-letter code groups, and they were sent this way via Morse code.

F7Z DE WN 1340 = 49 = XPH WRC =
RTXXF GXBZV GNOVX VFMKK
GIXMT SEFLM IVUFW IMG.

Crypto Simulation, *Cont. on page 10*

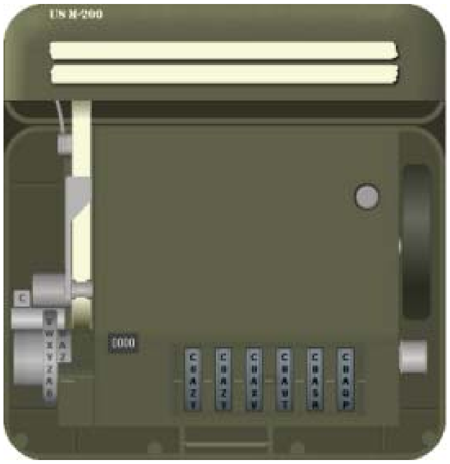
Crypto Simulation, *Cont. from page 9*

The first code group shows which codebook setting was used. (Note the column "Kenngruppen" in Screen 6.) The operator chooses one of the entries for that day and prepends two random letters to make a five-letter code group. Although this group is included in the word count, the receiver doesn't enter it. It sets the rotors to FWT and enters the coded message to produce the result, “PRESERVEWILDLIFEXPICKLE ASQUIRRELX”. Some punctuation could be represented as letter groups, but we'll skip over that in this quick introduction.

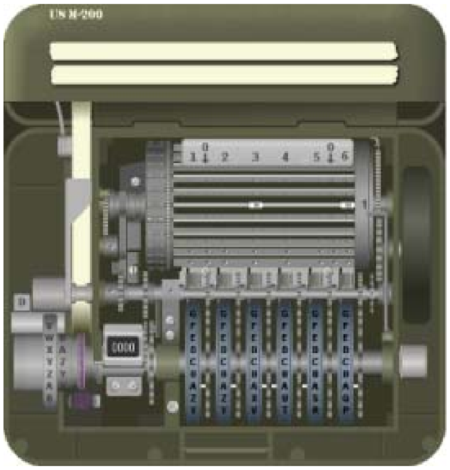
Hopefully, this brief discussion has given you some idea of what the Enigma really did. A few experiments with the simulator will make things much clearer, as will a few minutes spent exploring the Website.

Fortunately for the Allies, the Germans greatly overestimated the strength of their machines. Their primary error was in thinking that its construction was secret, when in fact the allies obtained working Enigma replicas from the Poles in 1939 and captured several during the war. In addition, some operators, especially in the Luftwaffe, were careless or poorly trained, and this allowed the British in particular to deduce codebook settings and changes in the equipment. Finally, many services used the same codebooks, and some, such as trawlers who were providing weather information in the North Atlantic, were vulnerable to capture.

The U.S. rough equivalent of the Enigma was the m-209—although it was known to be much weaker, as the Germans could decode its messages in about four hours. It was thus used only for tactical communications; strategic information was encrypted using other means. The m-209 was smaller (about 3 x 5 x 7 inches) than the Enigma, did not need a battery, and printed its output on paper tape, making it usable by only one operator. Besides being cryptographically weak, it was tedious to configure and slow to use. Despite these drawbacks, it was used through the Korean War and well into the 50s. Like the Enigma, you can buy models of the m-209, but a better approach is to experiment with a simulator from the same Website that has the Enigma simulator. Screen 11 shows the simulator view that an operator would see while using it.



Screen 11. m-209 Crypto Machine

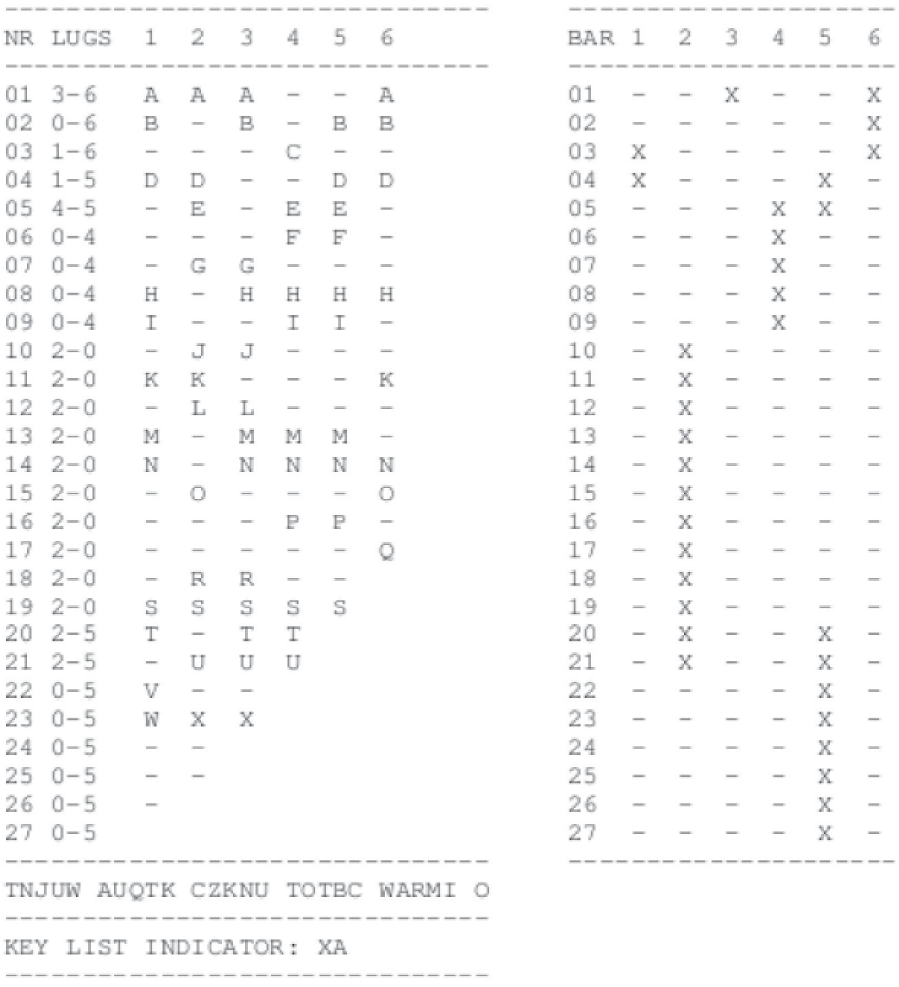


Screen 12. m-209 Crypto Machine Interior

Characters are entered by twisting the knob at lower left until the desired letter is opposite the index (A in this case). Then the black lever on the right is pressed. This advances the six rotors (visible at the bottom) and prints the output letter on paper tape (to the right of the input wheel). The simulator displays two tapes at the top; the upper one is a record of the input characters, and the lower one the output. The current output character is also visible just to the right of the input wheel (Z in this case). There is also a character counter (here showing 0000), and a round button to reset the machine. Finally, just above the input wheel is a tab marked C, showing the machine is in encrypt mode. This must be flipped to D for decoding.

You can get a hint of how tedious it is to set up the m-209 from its internal view, Screen 12 (above).

Screen 13. m-209 Configuration Table.



```
------------------------------           --------------------
NR LUGS  1  2  3  4  5  6                BAR 1  2  3  4  5  6
------------------------------           --------------------
01 3-6   A  A  A  -  -  A                01  -  -  X  -  -  X
02 0-6   B  -  B  -  B  B                02  -  -  -  -  -  X
03 1-6   -  -  -  C  -  -                03  X  -  -  -  -  X
04 1-5   D  D  -  -  D  D                04  X  -  -  -  X  -
05 4-5   -  E  -  E  E  -                05  -  -  -  X  X  -
06 0-4   -  -  -  F  F  -                06  -  -  -  X  -  -
07 0-4   -  G  G  -  -  -                07  -  -  -  X  -  -
08 0-4   H  -  H  H  H  H                08  -  -  -  X  -  -
09 0-4   I  -  -  I  I  -                09  -  -  -  X  -  -
10 2-0   -  J  J  -  -  -                10  -  X  -  -  -  -
11 2-0   K  K  -  -  -  K                11  -  X  -  -  -  -
12 2-0   -  L  L  -  -  -                12  -  X  -  -  -  -
13 2-0   M  -  M  M  M  -                13  -  X  -  -  -  -
14 2-0   N  -  N  N  N  N                14  -  X  -  -  -  -
15 2-0   -  O  -  -  -  O                15  -  X  -  -  -  -
16 2-0   -  -  -  P  P  -                16  -  X  -  -  -  -
17 2-0   -  -  -  -  -  Q                17  -  X  -  -  -  -
18 2-0   -  R  R  -  -                   18  -  X  -  -  -  -
19 2-0   S  S  S  S  S                   19  -  X  -  -  -  -
20 2-5   T  -  T  T                      20  -  X  -  -  X  -
21 2-5   -  U  U  U                      21  -  X  -  -  X  -
22 0-5   V  -  -                         22  -  -  -  -  X  -
23 0-5   W  X  X                         23  -  -  -  -  X  -
24 0-5   -  -                            24  -  -  -  -  X  -
25 0-5   -  -                            25  -  -  -  -  X  -
26 0-5   -                               26  -  -  -  -  X  -
27 0-5                                   27  -  -  -  -  X  -
------------------------------           --------------------
TNJUW AUQTK CZKNU TOTBC WARMI O
------------------------------
KEY LIST INDICATOR: XA
------------------------------
```

If you look carefully at the rotors, you can see small pins in the A row. Think of a pin to the right as a one and a pin to the left as a zero. The A row thus is set to 111001. However, setting the rotor pins is only part of the configuration. There are also 27 bars, each with two sliders that must be set. Here Bar #1 has been set to 36. Screen 13 shows a complete setup, typically used for one day.

If a letter appears, the pin in that row should be to the right (or set to 1); a dash indicates that the pin should be to the left (or set to 0). Note that rotor 1 has 26 letters, rotor 2 has 25, rotor 3 has 23, rotor 4 has 21, rotor 5 has 19, and rotor 6 has 17. The LUGS column shows the slider positions on each bar, and the table on the right also shows this, but in a different form. It's a real credit to our soldiers that they were able to perform this intricate configuration under combat conditions. I need several tries to do it at home, in an easy chair, with soft music and a cup of coffee.

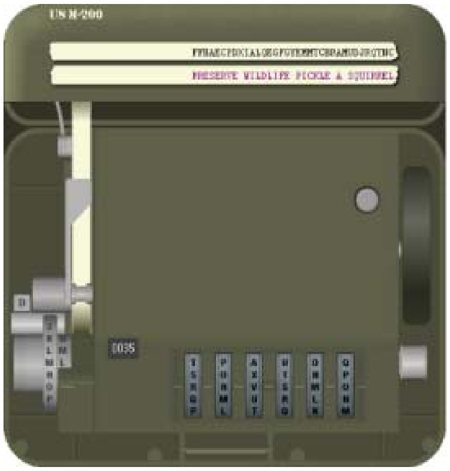
When complete, the operator would set the rotors to AAAAAA and encode 26 As. If correctly set up, the result should be the 26-letter sequence below the tables. Every configuration was assigned an indicator (XA for this one) that was attached to the encrypted messages, and the receivers used this to be sure that had their equipment properly configured.

Because it's so tedious and repetitive, I won't go through a configuration. Download and run the simulator if you want to experience this. I do think it will be helpful to run through encoding and decoding a message. For this, assume the machine is configured as described above. Like his German counterpart, the American soldier had to generate message key, and he used a similar procedure, encrypt the message and include an encrypted version of it with the message. Only if the receiver has an m-209 with the identical configuration can he recover the key to decrypt the message.

Again, we'll send the message, "Preserve wildlife. Pickle a squirrel." We choose CVQIMK, set the rotors to it and encode SSSSSSSSSSSS to produce IDJWE PNWFW XU, which will be our key. Our message will include both CVQIMK and SS, so the receiver can generate the same message key. Why 12 characters when we need only six? Recall that most of the rotors have fewer than 26 characters. In this case, when we go to set the machine, we'll find there is no W on rotor 4, so we'll just skip that letter. As a result, the actual key will be IDJEPN. The Americans replaced every space with a Z, but had no standard for punctuation. (If every sentence ended with "PERIOD," it would aid those trying to break into the messages.) We'll just eliminate the periods in this simple example. Our input becomes PRESERVEZWILDLIFEZ PICKLEZAZSQUIRREL, and produces FFBAE CPDXI ALQEG FGYEM MTCBR AMUDJ RQTNC. However, we have to add SS CVQIMK XA, where SS shows the letter we used to produce the key, CVQIMK is the setting to produce the key, and XA is the setup. We'll regroup these 10 letters to SSCVQ IMKXA, because encrypted messages always appear as five-letter code groups. We'll also repeat this important information at the end of the message. Thus, the complete message becomes the following.

SSCVQ IMKXA FFBAE CPDXI ALQEG FGYEM MTCBR AMUDJ RQTNC SSCVQ IMKXA

The receiver uses an identical procedure to develop the message key. That is, he sets his rotors to CVQIMK and encodes SSSSSSSSSSSS to produce the message key. He too has to discard a W. He then flips the code/decode tab to D and enters the encrypted message. Screen 14 shows the result.



US M-209

FFBAECPDXIALQEGFGYEMMTCBRAMUDJRQTNC

PRESERVE WILDLIFE PICKLE A SQUIRREL

Screen 14. m-209 Simulator in Use.

Note that the m-209 has replaced Zs with spaces. They would also be replaced in such words as "zero," but this would be evident from the content.

A little experimenting with these simulators will reward you with a better understanding of the difficulties of communicating securely before the computer age.

Dick Maybach *is a member, Brookdale Computer Users' Group, NJ (www.bcug.com; n2nd (at) att.net)*

This article appeared in the September 2016 issue, BUG Bytes, and is distributed for reprint by APCUG member groups

Capital Campaign to Renovate the Resource Center

We are lucky to have this community of people who are interested and skilled at computers and technology. Only a few cities in the United States have an award-winning computer society as active as DACS! Thank-you to the many people who freely give their time to present at our General Meetings, teach at our SIG Meetings, serve on our Board, and help organize events. We are an all-volunteer organization.

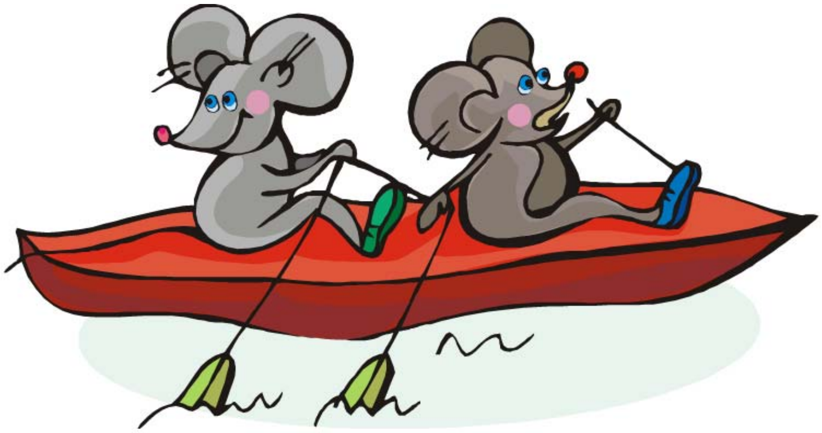
We are launching a capital campaign to renovate our Resource Center, where we hold SIG meetings and other events. We are fortunate that the city of Danbury has for 20 years provided this space for us at no cost in a city-owned building. However, the space needs renovations, including rug replacement, paint, moldings, and new chairs. We cannot afford new rug, but we already have a promised gift of lightly used rug from Meadow Ridge, a retirement community to Redding. We have also lined up skilled volunteers to install the rug, paint, and do other renovations. All we need is some money for materials.

Our goal is $1,500. Please consider a gift to DACS! We are a 501(c)(3) organization, and your contribution is tax-deductible.

You can make an online donation at our website www.dacs.org or mail a check to:

DACS, Inc.
c/o Bert Goff, Treasurer
65 Legion Rd.
New Milford, CT 06776

dacs.doc
Danbury Area Computer Society
65 Legion Rd
New Milford, CT 06776



When you come to the next DACS meeting,
why not bring a friend?

Future Events:

February 7

David Fischer
Online Marketing

March 7

TBA

April 4

TBA

May 2

TBA