Access

Newsletter of the Louisville Computer Society
Kentuckiana's Macintosh Users Group **August 2005**

I've Got a Secret: Part I
by
Lee Larson

One of the recurrent questions on the MacGroup email discussion list is "What are those public keys that are littering my keychain?" This is the first of at least two articles explaining what's going on. This first article is a gentle introduction cryptography.

Encrypting messages is an ancient idea. Thousands of years ago Julius Caesar sent his messages using what we now call a Caesar shift cipher. He just shifted the alphabet a few characters and removed spaces to produce seemingly nonsensical text. For example, with a shift of 4, *a* is replaced by *e*, *b* by *f*, and so on. The text of this paragraph, with a shift of 4 and written in blocks of 5 might look like this:

```
IRGVC TXMRK QIWWE KIWMW ERERG MIRXM HIEXL SYWER HWSJC IEVWE KSNYP MYWGE IWEVW IRXLM
WQIWW EKIWY WMRKA LEXAI RSAGE PPEGE IWEVW LMJXG MTLIV LINYW XWLMJ XIHXL IEPTL EFIXE
JIAGL EVEGX IVWXS TVSHY GIWII QMRKP CRSRW IRWMG EPXIB XJSVI BEQTP IAMXL EWLMJ XSJEM
WVITP EGIHF CIFFC JERHW SSRXL IXIBX SJXLM WTEVE KVETL AMXLE WLMJX SJQMK LXPSS OPMOI
                                        XLMW
```

Many of us played with similar ideas when we were children. Most of the "Captain Crunch decoder rings" and other such toys are based on something like a Caesar code. All the schemes where one letter is replaced by another are called substitution ciphers. Edgar Allen Poe used a substitution cipher in his 1843 mystery, *The Gold Bug*. Poe's story is interesting because it also points out the weakness of substitution ciphers: the frequency of letters in English text allowed the mystery to be solved. The letter that appears most often is probably the substitute for *e*, the second most often is the substitute for *t*, and so on. Breaking a substitution cipher is tedious work for a person working only with pencil and paper. With a computer, there's little challenge because the computer can count letters almost instantly.

Throughout history there has been a long battle between those who code messages and those who want to read them. Most knowledgable people agree that the subject doesn't really get interesting until World War II, when technology took over. It's almost impossible to tell apart the fact and fiction swirling around the story of Bletchley Park, Alan Turing and the German Enigma Machine. But, when you get right down to it, the Enigma Machine was nothing more than a really sophisticated Captain Crunch ring that could change the substitutions as it coded.

The problem with all ciphers is the need for a *key*. The key is a method to uncode the code. Caesar might have told his generals to shift by 4, and the Germans had top secret key books that told how to set the Enigma Machine to read or write a coded message by a certain person at a certain time. Both the coder and the reader have to share a key to make the code useful. If the key becomes widely known, then the code is useless.

After WWII, encryption became a study for mathematicians, and sophisticated computational methods were developed to tease information from cleverly encoded text. At the same time, methods were developed that were actually mathematically proved to be nearly impossible to crack, based on current mathematical knowledge. Most of these relied on mathematical algorithms that are easy to do, but very hard to undo. For example, 6133*9733=59692489, and this is the only way to write 59692489 as a product. (Using 1*59692489 is not considered sporting.) The multiplication is easy, but factoring 59692489 is a lot harder. (If you don't think so, then factor 3205073296037 as the product of two positive integers, both greater than 1.) It's not hard to come up with numbers that the fastest computers would spend centuries factoring.

[1] A good book on the subject is *The Codebreakers* by David Kahn.

Secret: Con't on Page 4

Meeting at 6010 Preston St

Louisville Computer Society, Inc.
P. O. Box 9021, Louisville KY 40209-9021

Access is a service mark of the Louisville Computer Society, Inc. Our newsletter is publisher monthly as a service to Macintosh users. We are dedicated to the education and benefit of Louisville and southern Indiana computer-oriented communities.

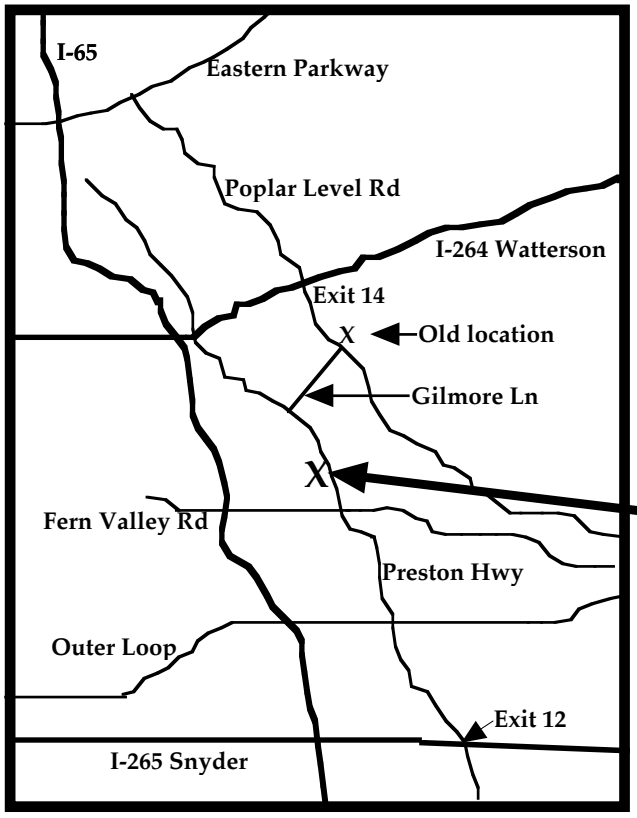
Subscription rate is $26 a year; it is mailed free with your membership in LCS, a Macintosh Users Group (MUG).

For more information write to the above address or call 502-363-3113 between 5 and 9 P.M. only.

Come to our monthly meetings

The Louisville Computer Society meets the 4th Tuesday of each month, 7-9 P.M. (except December) at Pitt Academy, 6010 Preston Hwy. (1 mile south of Gilmore Lane on Preston St.), Louisville KY 40219 (see map below).

Pitt Academy's new location is 0.4 mile north of Fern Valley Rd. or 4 miles north of I-265 on Preston Hwy. The school is directly opposite Town & Country Ford which has a LARGE American flag flying.



Business and Financial News at Forbes.com

Forecast for Apple Computer
http://www.forbes.com

IPod Mini With Color Screen Would Be 'Home-Run Product'

Piper Jaffray maintained an "outperform" rating and $52 price target on Apple Computer (nasdaq: AAPL - news - people), expecting the company to launch a number of new products by the end of 2005.

Products that are likely to be available include a higher capacity iPod Shuffle and color screen iPod mini. "In our view, a color screen iPod mini would be a home-run product for Apple in the upcoming holiday season." Piper sees these new gadgets being formally introduced at Apple Expo in Paris, which runs from Sept. 20 to Sept. 24.

"[W]e expect iPod to continue to be a foundation for growth in other parts of Apple's business, and we expect that by the end of calendar 2005 more than 35 million iPods will have shipped, providing Apple with a greater scope of awareness for various products. It appears that this phenomenon has begun to take effect, with 1.18 million Macs shipped in the June quarter."

The research firm noted that a few products will not be seen this year, including a video iPod and a new Mac. "We do expect Apple to periodically bump up the speed of the existing Mac product line, but we would be very surprised to see any brand new Macs released into the market prior to the start of the Intel (nasdaq: INTC - news - people) integration in mid-calendar 2006."

Our new location

If you wonder how to get there, pretend you are leaving the parking lot at the old location where we have been meeting: Go straight across the intersection onto Gilmore Ln. Drive approximately 1 mile to the first traffic light at the other end of Gilmore. Turn left onto Preston St. Go through three traffic lights. (~1 mile) and turn RIGHT opposite the LARGE American Flag flying in front of Town & Country Ford auto dealer.

Pitt Academy
6010 Preston St.

If coming from the South, Pitt Academy is 0.4 miles north of Fern Valley Rd. It will be on your left, just after you cross over the drainage ditch.

Plenty of parking space. Enter the building and turn right. The computer lab is about the second door on the left.

LCS e-mail address book

Andrew Arnold	**a0arno01@athena.louisville.edu**
Jim Bennett	**bennetts29@insightbb.com**
Anne Cartwright	**cartwrig@aye.net**
Marta Edie	**meld@insightbb.com**
Jonathan Fletcher	**jfletch@newmediaconstco.com**
Bernard Griffins	**latigopc@bellsouth.net**
Tom Guenthner	**Tom@aye.net**
Nelson Helm	**helmkyny@clockwinders.net**
Glenn Hoehler	**glenn@insightbb.com**
Harry Jacobson-Beyer	**harryjb@bellsouth.net**
Bill King	**bk0413@insightbb.com**
Lee Larson	**leelarson@mac.com**
Jeanie Montgomery	**jerryandjeanne@aol.com**
Tympana Oberhausen	**tympana@bellsouth.net**
Brian O'Neal	**iMac@mac.com**
Ed Stirrers	**stivers1@earthlink.net**
Jan Webber	**kyjweber@mac.com**
George Yankee	**jeffco13@bellsouth.net**

If you wish to be added, contact cartwrig@aye.net

The work goes on at Pitt Academy
August 9, 2005

Brian O'Neal

LCS Web Page, List Serve & Officers

Web Page	**www.kymac.org**
List Serve	**macgroup@erdos.math.louisville.edu**
Tom Guenthner, President	**Tom@aye.net**
Lee Arson, Vice President	**leelarson@mac.com**
Bill Rising, Program Director	**braising@louisville.edu**
Brian O'Neal, Web Master	**iMac@mac.com**
Anne Cartwright, Newsletter Editor	**cartwrig@aye.net**

Upcoming Programs 7 P. M. at Pitt Academy on Preston St. (see map on page 2)

August 23 **Lee Larson** Watch When You Want -- MythTV -- TiVo without Fees or Ads.

September 27 **We need suggestions for future programs!!!**

October 25

If you have any suggestions or special requests, please contact Bill Rising at **braising@louisville.edu.**

Special Interest Groups (SIGs)

SVI-SIG is the Still & Video Imaging - Special Interest Group. This SIG is devoted to manipulating pictures, both photos and movies. It meets the second Tuesday of each month, 7 PM at Pitt Academy. **Next meeting September 13** at the new location.
Meetings are very informal and open to anyone who shares our interests. Any particular focus you want our meeting to cover?
For more information contact Bill King at **bk0413@insightbb.com**

Louisville Computer Society
Macintosh Users Group
Membership Application

Please send your $26 check for a year's membership, made out to Louisville Computer Society to:

Louisville Computer Society
P.O. Box 9021
Louisville,KY 40209-9021. **Thanks! See you at the next meeting.**

Fill out the following ; clip on the dotted line (or copy to another piece of paper) and send in with your check .

❑ New or ❑ Renewal Membership

Name: _____

Home Address: _____

City: _____ **State:** _____ **Zip+4:** _____

Home Phone: (____) -- _____ **Your E-Mail:** _____ **Your Home Page:** _____

How did you hear about LCS" _____

Secret: Con't from Page 1

These modern mathematical methods still share one weakness with the older substitution methods: the key. You still had to share a key with whomever you wanted to read your messages. In 1976, two American mathematicians, Whitfield Diffie and Martin Hellman, introduced an ingenious new idea called *public key cryptography* that removed this weakness and ushered in the modern era of encryption.

Here's the gist of the idea. Suppose Alice has a safe with two keys: if one of the jeys locks the safe, then only the other can unlock it. She gives Bob one key keeps the other one private. When Bob wants to send her a private message, he puts it in her safe and locks it with the key she gave him. Only Alice can read the message because only she has the key to unlock the safe. If Alice puts a message in the safe and locks it with her key, only Bob's key can unlock it, so Bob knows the message came from Alice.

The same thing is done mathematically with public key cryptography. Every user has two keys: a public key and a private key. (Actually, they're just large numbers.) The public key is given away to anyone. When a message is encrypted using the public key, only the holder of the private key can read the message. This is where the keys come from in your keychain; they're the public keys of a public-private key pair. For example Jerry Yeager's public key is

```
BB 1C 2C DC 10 18 59 23 68 4F F7 1B 73 66 E7 5F C2 CC 0A 68 45 FA BC DD 5A 89 5E CA 50 F8 D0 E2 27
D4 81 7D 2C 75 DA D9 3D 1B 4E 5C 60 DD DB D9 63 D5 DE 16 BD 47 67 9E BF 28 92 90 1C D7 19 AF 39 DB
FD 56 31 74 14 9C B5 4D E3 D8 34 7C E4 A5 99 C9 CD 36 A3 8C 3B 2D A1 10 4C 10 7F A0 E3 98 A2 77 D6
CA 1F 15 48 20 ED 81 EC 80 27 88 F1 67 E7 35 6E 5B 1C 87 0C ED 49 6F 0C BB 02 1F 06 C6 28 87 C9 5E
33 24 9E F8 85 5B B4 29 0D 44 10 D6 17 2C 60 21 A8 8F C1 FD FC 21 E1 40 E0 CC 2B B5 83 77 1C C6 C8
55 42 59 1A 19 B4 0C EE 99 37 D5 CF 2D F6 15 F3 CF 28 22 52 AB 73 FB 12 DB 5E EC 48 71 FA 12 8C CD
4B BC 1F DD 2B 22 47 DE 4B 5E 29 79 3E BF 00 50 71 1D D5 B9 65 BA 10 5D 21 4F 9E 3D E4 BC 5F BA 57
12 F2 6D 16 54 3A 2E 41 AA 86 E1 4B F6 A2 ED 6A DA F6 26 77 71 67 36 D5 4B
```

It looks strange because it's an integer written in base 16 divided into blocks of two characters.[2]

If Jerry encrypts a message using his private key, only his public key can decode the message. Anyone receiving the message has a way of checking whether the message actually came from Jerry. This is the idea behind the *digital signatures* some of us use on our email.

The next article will contain more details about how to use these ideas in Mac OS X.

[2] ~~It's equal to the base 10 integer~~

```
23620456753818697974756022699661454276211343497904214294281242189655810069347 6\
28725703751142197677351874163825752405685165332974543483661138723792814309001 2\
40294804085998610086525373340963083417585554426667826789843983294542942742558 5\
04851666896388014019910130734636552259973294456150791461624570251643751372620 4\
67336955005919980881671213341544375995260355633509596970725264795712629849317 5\
99887979488530884368084579647469158508835792727823334692005509379411508691705 6\
47788384193018207392799447237528678493016605293336904450575277936166557315058 1\
60898730904697849616264645333316170558061468330307922389626477948097867
```

August 23 meeting will be at our new site.
See Page 2 for directions.

Louisville Computer Society
www.kymac.org
Macintosh Users Group

The Louisville Computer Society
P. O. Box 9021
Louisville KY 40209-9021

37¢

Mailing Label