Coffee and Computers
Newsletter

Volume 2, Number 2 **February 24, 2002**

STRONG ENCRYPTION

A funny thing happened at 'Coffee and Computers' on a recent Friday. I got called to task for NOT "building a watch." Let me try to remedy this omission.

The question I ducked had to do with "Strong Encryption." Somebody wanted to know what it meant when a web site said it was using "128 bit" encryption.

The answer is a little complicated, but here goes.

Computers use ENCRYPTION to scramble data that you, the user, don't want an outsider to be able to read. This may be a transaction with your stockbroker. It may be when you send your credit card information to Amazon when you buy a book. It could be used in email when you only want the recipient to be able to read your message. Most of the time encryption takes place automatically in your computer so you don't need to initiate anything. You may see a small key or lock symbol in the taskbar when your computer is using encryption. How does encryption work?

Computers operate inside using a system called "BINARY." This means that everything works like a bunch of switches. Things are either ON of OFF. In computer terms, everything works by interpreting ONE's and ZERO's. A ONE means something is ON and a ZERO signifies that something is OFF. There just are TWO STATES: ONE or ZERO. Computers call these one's or zero's BITS.

Let's look at this like a CRYPTOGRAPHER. One bit can be either a one or a zero. Thus one single BIT has only two possible COMBINATIONS: 0, 1.

How about two bits? It can have FOUR possible combinations: 00, 01, 10, 11.

If we remember our high school math, these binary combinations can be expressed as POWERS OF TWO. Thus the four combinations of two bits are two times two. Three bits can have two times two times two, or eight possible combinations. Four bits have sixteen combinations: 0000, 0001, 0010, …. Finally, eight bits (a BYTE) has 256 combinations, etc. You can see that the number of combinations grows rapidly.

A cryptographer can scramble a message 256 ways using eight bit encryption. One of the eight possible combinations is used to form a KEY. A KEY is used to ENCRYPT a message and the recipient needs the same KEY to DECRYPT the message. This is like the Jack Armstrong Magic Ring. Both parties needed the same key to send and receive secret messages.

Someone intercepting this secret message only can BREAK the code by trying all possible combinations, hoping to find the correct key.

Obviously, with a fast computer, trying all possible combinations of eight bits wouldn't take much time at all to find the correct KEY and BREAK this code.

So, how do we make it very hard for even the best cryptographer to unscramble our messages? We use many more than eight bits to form our key. In fact, we use 128 bits. Thus "128 bit" encryption!

To attempt all possible keys, we must launch a BRUTE FORCE ATTACK on the message. But 128 bit encryption has two times two times two multiplied 128 times. This is a very large number and thus a very large number of possible combinations. In fact, the number is about 3 followed by 38 zero's. This may be more than all the stars in the universe.

To attempt a brute force attack on a message encoded using a 128 bit key would require that a computer try all possible combinations until it finds that one single number that makes sense out of the encrypted message.

Mathematicians and computer scientists have projected that even using the most powerful current computers and those contemplated in the next 20 to 100 years, it would take years to find the correct key and decrypt our message.

Are we safe? That depends. It is possible that a very smart cryptographer could develop a smarter way to decrypt our message without launching a brute force attack. This depends upon the method (algorithm) we use to encrypt our message even with our 128 bit key.

However, using current encryption methods and 128 bit keys, no-one has come up with a good way to decrypt our message without having the correct key. We probably are safe!

I hope you haven't found this too confusing. And please keep coming up with interesting questions.

See you Friday's.

Art

P.S. Thank Lousie Records for coming up with the format for this newsletter using columns instead of tables. Take her word processing class for details.