TECH TALK

The magic words are "squeamish ossifrage" or Alice, Bob, and Eve

BY ALEX FLAXMAN, MD, MSE, *BETH ISRAEL MEDICAL CENTER/ALBERT EINSTEIN COLLEGE OF MEDICINE, NY - EMRA TECHNOLOGY COORDINATOR*

That is "Alex" in the Pigpen cipher, once used by the Freemason's and still used by children. If an encryption method once secure enough for the Freemasons has been relegated to children, how could one ever hope to protect, for instance, patient records?

In other words, how can we securely encrypt? Monoalphabetic substitution ciphers, where each letter is replaced by a different letter (or symbol, as above), first referenced in the Kama Sutra and first used militarily by Julius Caesar, were broken in the ninth century with a technique called "frequency analysis." Stronger encryption methods such as misspelling words or spelling words phonetically (eg "enfarkshawn" instead of "infarction") before encryption, are also easily broken using frequency analysis with additional techniques. Other ciphers throughout history, even some languages completely lost except in print (eg Egyptian Hieroglyphics, Linear B) have been deciphered. The only encryptions believed to be secure today are RSA and the Diffie-Hellman-Merkle method. The Diffie-Hellman-Merkle method requires two systems to converse in real time so RSA is the system in widespread use.

"...the sender is secure that, even if intercepted, no one but you can read the file."

RSA works on a key system. Your computer file (the patient's record, in this case) is encrypted according to your "key." The key is split into two: your "public key," available to everyone, and your "private key," kept to yourself. Anything encrypted by your public key can only be decrypted with your private key, and vice-versa.

If someone wants to send you something they first encrypt it with your public key. It can now only be decrypted with your private key. So the sender is secure that, even if intercepted, no one but you can read the file. For *us* to send a file to *someone else*, we must encrypt the file with *their* public key before sending it.

As an added bonus, we can first encrypt the file with our private key then with the receiver's public key. It must first be decrypted with the recipient's private key (protecting the file from interceptors). The resulting message then needs to be decrypted with our public key. That proves the file must have been encrypted with our private key, which means only we could have sent it. We *digitally signed* the file.

These are the basics of encryption. We can send our credit card information to eBay, a patient's information to a remote hospital, and a private doctor can send a patient's EKG to the ED. We know who sent the file and, even if intercepted, that no one else can read it.

CONTEST: WHAT'S UP WITH THIS HEADLINE?

The author will send a bottle of white or red wine to the first person to e-mail the correct explanations of both references headlines. Contestants must be EMRA members, over 21, and consent to have their name and program printed in a future issue of EM *Resident.* You are not allowed to ask non-EMRA members for help (you're on the honor code for that one). Send entries to aflaxman@emra.org. Not responsible for late, lost, or misdirected replies. The author's decision is final. ■