College of Saint Benedict and Saint John's University

DigitalCommons@CSB/SJU

Forum Lectures

Forum

1-29-2015

Online security, cryptography, and quantum computing

Lynn Ziegler
College of Saint Benedict/Saint John's University, lziegler@csbsju.edu

Online Security, Cryptography, and Quantum Computing

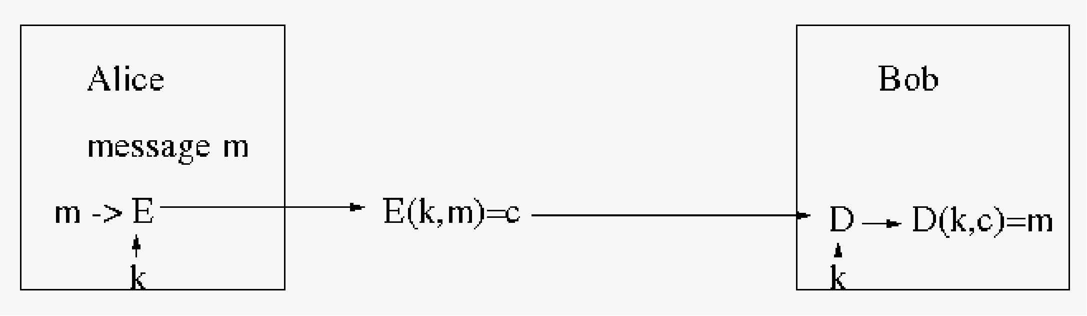
Disclaimer: I spent part of my sabbatical last year working for an NSA subcontractor so I cannot talk about my work there. (Top secret clearance, etc.) This talk is taken entirely from material I already knew or learned after my work with the subcontractor. This may mean that I cannot answer some questions.

Secure online sites – https://

- Internet sites starting with https:// are designed to allow you to do secure transactions online. The idea is that the information you exchange with the site should be secure from evesdroppers.
- The security is maintained by **encrypting** the information exchanged. This means that the information transmitted is first "scrambled" in such a way that it should be indecipherable by anyone except the sender and the web site.
- Such transactions are done via a symmetric cypher. This cypher consists of a encrypting function E and a decrypting function D. Both of them work using a random key k. We write E(k,m) and D(k,m) where k is the common key and m is the thing being encrypted.

Alice and Bob

- For historical reasons, cryptography experts have consistently used the names Alice and Bob to illustrate encryption/decryption. Here is how Alice would send a message to Bob with symmetric encryption.



- Notice that the idea is Alice encrypts m with E and k to get cyphertext c and Bob decrypts cyphertext c with D giving the original message m.

Symmetric Cyphers and Keys

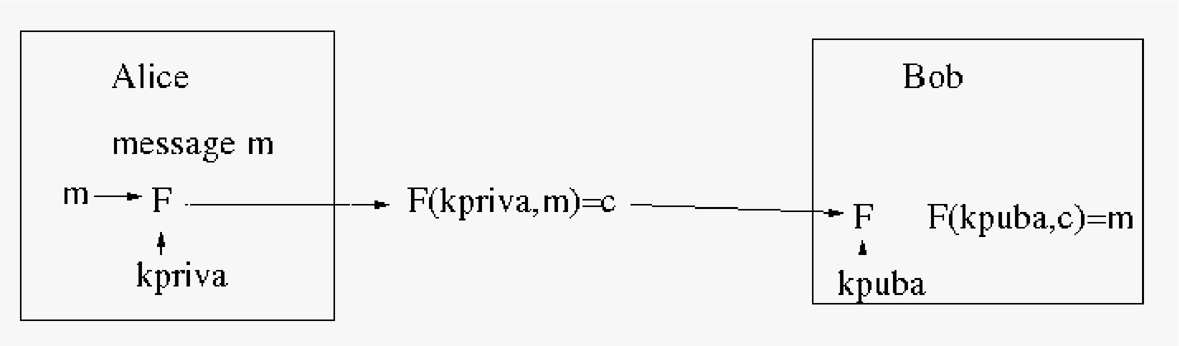
- Note from the illustration on the previous screen that the key k must be known by both Bob and Alice. (Everyone, generally, knows functions E and D.) k **must be kept secret!**
- Generally, even if someone intercepts many messages they will not be able to decipher the cyphertext c unless they know k. (Actually, the correct thing to say is that the probability that they can decipher cyphertext c or discover k is very low.)
- This means that Alice and Bob (or you and the https:// site) need to securely share the key k!
- Even large institutions like international banks and governments do similar kinds of things and must share keys.

Key Exchange

- In 1977, Ron Rivest, Adi Shamir and Leonard Adelman introduced the first public-key encryption system which was named RSA after their last initials.
- Public-key encryption systems work somewhat differently. There is only one function, F(k,m), which is known to everyone. Each person has two keys: a public key (**kpub**) and a private key (**kpriv**). Each person or program has their own public and private keys. (For Alice and Bob we would have (**kpuba**, **kpriva**) for alice and (**kpubb**,**kprivb**) for Bob.)
- The function F(kpriv,m) and F(kpub,m) are inverses of each other for each pair of public and private keys.

Public Key Encryption – Alice and Bob return

- The important thing about public key encryption is that even knowing the public key it is VERY hard to find the private key. This means that everyone can publish their public key and not care if someone "bad" gets it. Given this, Alice and Bob both know Alice's public key. We can then have Alice send a secure message to Bob in this way:



- Note that Bob even knows Alice sent it if Alice is the only one knowing her private key.

Facts about RSA

- It is known that you could break RSA encryption if you could factor very large numbers – that is, numbers with 600+ digits for RSA 2048 or 1600+ digits for RSA 4096. All known computer programs for doing this are enormously slow – generally they would take years to do this.
- Wait: If RSA is so great why deal with symmetric cyphers at all? The answer is that encryption of messages with RSA is very slow. Thus RSA is generally reserved for exchanging keys. Thus, before Alice and Bob start sending messages, one of them – say Alice, first encrypts a symmetric key k with kpubb (Bob's public key) and posts it in a public place where Bob can find it. Bob then decripts it with kprivb and now Alice and Bob both have the key. (The same thing happens if you talk to an https:// site. The site sends you their public key and you randomly pick a symmetric key, encrypt it with that public key and send it to the site so you both have the same symmetric key.) (Actually, there is also certificate verification.)

So it sounds like everything is fine

- Physics steps in and spoils everything. (Just joking – I like physics even though I am far from being a physicist.)
- There is such a thing as a quantum computer. The advantage quantum computers have is that for certain kinds of calculations, quantum computers can be set up to do a VERY LARGE NUMBER of computations simultaneously.
- A man named Shor developed an algorithm for quantum computers that would factor very large numbers in reasonable time. (Depending on the size of the number and the speed of the quantum gates, perhaps in minutes, hours, or a few days.) (It turns out his algorithm also solves the discrete logarithm problem which breaks another key exchange mechanism called Diffe-Hellman.)

Are we doomed???

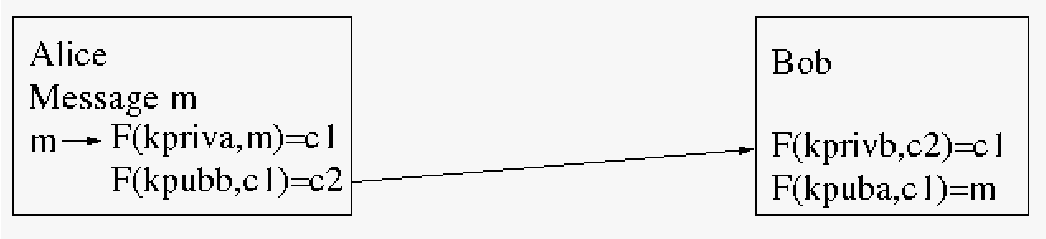
- Maybe – but not for a while. Currently the kind of quantum computers that have been built are small. Quantum memory units are called qubits and the largest quantum computers capable of running Shor’s algorithm only have about 20 qubits. (A Canadian company called DWAVE has a quantum computer with 512 qubits but it has very high error rates on its qubits and is based on another principle called quantum annealing.) To run Shor’s on 2048 bit RSA would require at least 10,000 qubits. It will probably be a while before such a machine can be built.
- There is a third key exchange mechanism using elliptic curves that Shor’s algorithm does not solve but most people believe a similar kind of algorithm will be developed for elliptic curve key exchange on quantum computers. (This will, however, buy us some time since you will need larger quantum computers for elliptic curve key exchange.)

Physics to the Rescue!

- No more physics bashing.
- The quantum computer is based on principles of quantum physics which is an extremely well verified scientific theory. It is fairly certain that quantum computers of any size can be built eventually. But…
- Physics also has a potential solution called Quantum Cryptography which can be used for exchanging keys. It is provably secure. That is, if you follow one of the methods of sending a key over a transmission line with Quantum Cryptography it cannot be intercepted since interception implies measurement which changes the transmission and the key exchangers can detect this. Its only problem is range. So far the longest distance has been a few kilometers. This may be the method of the future.

A Bit of Fun

- Public key encryption can also do some amazing things. Again suppose that Alice and Bob have their keys, kpuba, kpubb, kpriva, kprivb and Alice wants to send a message to Bob in such a way that only bob can read it and only Alice could have sent it.



- This is called a digital signature. The only way Bob gets a readable message is if Alice used her private key and only Bob can read it because it needs Bob’s private key to decipher it.