Quantum cryptography

James Peach

October 29, 2014

1 Cryptography

There are many applications of cryptography in technology from banking to gaming. The ability to perform communication between two parties without the ability for others to listen in on the conversation allows some activities like sending money faster and opens up the possibility for new things that were not possible before, like the ability to share your work with others and for them to know that it was you that produced the document.

Crypotography allows us to do all this and more! There are lots of different types of cryptography: * Hashing algorhtyms * Symetric (secret) key crypto * Antisymetric (public) key crypto these all have very different uses and all do verry different things.

1.1 Hashing algorhythims

This family of crypto algorithyms are an effective method of turning a input message of bytes and producing an output of a static length so using MD5 as an example of a hashing algorythm on the binary conversion of the string "Hello world!" produces the output

"86FB269D190D2C85F6E0468CECA42A20"

this is a 16 byte hex string. now the usefullness of a hashing algorythm is that if you change the input message the output or digest as it is known is vastly different if we use a message of "Hello world?" instead the digest is

"48604754B9FED84B3FEEB84C5DC138C0"

this property means that if i was sent a very large message and its digest, i could very easily see if we both had the same message by comparing the digest. even one mistake in the message will produce a completley different

digest. now of course the number of different messages is infinite however given the example of MD5 with its 128 bit digest you *only* have $3*10\hat{3}0$ possible hashes. this means that there will be some messages that have the same digest. this is a problem, consider you downloading a program allong with the hash from a software company, you only want to run the program if you can be sure that the program you have is exactly the one that was sent because if you instead run a program and it turns out to be a virus your boss will be very angry. if there was an easy way to create a program with the same digest then it could be possible to fool you into running the attackers program when two such messages both have the same digest this is called a hashing collision. the effectivness of a hashing algotitym is the combination of a small possibility of collisions and a quick calculation speed.

1.2 Symetric key cryptography

as the name suggests symetric key crypto is the process of encrypting a message with a key or locking it. this prevents anyone without a key to read the message. this allows the message to be passed through a third party (in most cases the internet) to an intended recipient who has a symetric (identical) key to the one you used to encrypt it. this type of encryption allows large amounts of data to be sent securley however the problem with this is that both parties must have agreed on a key before needing to send a message. they must have a secure way to do this, they could have a list of keys that they both use that was passed between them without a third party having access to the key i.e. on a private network. it should not be possible to find the key for an encrypted message from simply examineing it no matter how long the data.

1.3 Antisymetric key cryptography

this is similar to the above symetric key cryptography, however the interesting part about this is in the key pair. when a key is generated from a random seed the algorythm creates two. one is chosen as the public key and one as the private key. the public key is put on display by a trusted thrid party the private key is never publicly visible and no one but the creator has access. both keys can encrypt a message however once a message has been encrypted only the other key can decrypt it. this has two main implications: * any file can be secureley sent to the (private) keyholder by encrypting the file with

the public key. this ensures that only the keyholder can access the file * the keyholder can hash a file and then encrypt the hash with the private key. this has the effect that anyone can verify the file to ensure that the creator has indeed had access to the original these techniques allows applications to ensure that they can trust that a user is indeed the creator of the message. for example the git server verifys that the commit has not been tampered with by anyone on the network and that the user was indeed the author of the commit as no one can create a signed file without the private key. the opposite is also usefull. your bank may publish their public key and a digital signature with every web page or document. your computer can then verify these documents were indeed created by the bank and no one between has tampered with them.

2 Quantum computing

The advent of quantum computing means that the flaws discussed in the processes above could be easily found and the gaurantees they give cannot be trusted. Third parties could listen in on private conversations. files and pages on the internet cant be trusted or verified. this is possible because with classical computation the effort required to break these gaurantees is so impossibly large that the in the age of the universe not a sinlge one could have been broken. however quantum computers offer techniques that were before impossible classical computations can be made many orders of magnitude faster and things that were before impossible, possible

2.1 Quantum cryptography

Quantum cryptography is an effort to offer the above prinipals but instead of offering security by mathematics, quantum cryptography bases the security on quantum perculiarities that once proved will not offer any possible way around them given any amount of computation available.

one such quantum perculiarity is the spin states of photons. The spin of a photon is in one of 4 directions up-down, left-right top-left-bottom-right, top-right-bottom-left. the quantum nature of the photon means that you cannot mesure a photon without disturbing it. and you can only mesure one set of directions at a time if you mesure with a non-diagonal set of detectors then you will only get a correct answer if the spin is in one of the two states

you chose to mesure otherwise you get a random incorect answer and you cannot mesure a photon twice.

lets consider two parties Alice and Bob, Alice wants to send a message to bob without anyone knowing what was sent. Alice will use standard symetric key encryption however to send the key she will encode a string of photons with different spins and send them to bob. in order for bob to decode the photons he will set up his detector in one of the two positions. he will incorrectly mesure half of the photons however once he has made and recorded the results he sends a list of the detectors that he used for each mesurement to alice. alice simply replies with the mesurements for which bob used the correct detector. Bob then removes the incorect mesurements and this leaves a list of values that can be used as a key for standard encryption. because of the properties of the quantum behavure of the particles any eavesdropping and mesurement of the photons will lead to a message bieng unable to be decoded by bob. this will lead to alice and bob knowing that thier message was comprimised.

now both parties have access to a collection of random bits, the same bits in the same order. and we also have the physical knowlege that is is impossible for anyone inbetween to get the code. when both parties have these then this key can be used in a traditional method to encrypt any data. the secret to having this form of encryption work is having a large key. more traditional methods for key distribution rely on other forms of encryption for example first encrypting the key with a public key and then sending the encrypted key publicly. the quantum method is more secure and dosent́ rely on a less secure method to transport the key.

3 Conclusion

Cryptography has been arround scince before the internet and has been an ever evolving science with a basis on mahematical properties and computational complexity. however the quantum revolution has changed this ever changing and breaking cycle of new algotithms into a more static and proved method. of course at the moment only the key is transfered over the new priniple however in the future the whole process can be secured in this way and then we should be totaly safe from the prying eyes of others.