Quantum cryptography

James Peach

November 2, 2014

1 Cryptography

Cryptography is the science of information security. Security can take many different forms. Encrypting your new secret document so that only you can view and change it. Or methods for proving the authenticity of a document while allowing others to view it and distribute it. With many more applications being created every day its no surprise that there are more and more things that need to be secure. everything from the designs for your latest processor to your bank balance, there needs to be cryptographic backing for all these applications to be successful.

There are many applications of cryptography from secure websites to gaming. The ability to perform communication between two parties without the ability for others to listen or gain information allows activities like sending money through an on-line website in just a few clicks 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.

Cryptography allows us to do all this and more! There are lots of different types of cryptography:

- Hashing algorithms
- Symmetric (secret) key cryptography
- Antisymmetric (public) key cryptography

All of these have very different uses and all do different things.

1.1 Terminology

Message - This is typically a varying blob of data, this could be a string of characters or an collection of bytes. This is the data you wish to encrypt.

Digest - This is the result of a hashing process. The size of the digest is usually a fixed length for any given algorithm, many algorithms have different variations on the length of the digest.

Plain-text - This is similar to the Message above however plain-text is usually the input to an encryption algorithm

Cipher-text - This is the output of an encryption algorithm, this is not human readable text and can only be deciphered with the key used to encrypt it.

1.2 Hashing algorithms

This family of cryptographic functions are an effective means of taking an input message of bytes and producing an output digest. For example using MD5 (a hashing algorithm) on the string "Hello world!" produces the following output:

```
86FB269D190D2C85F6E0468CECA42A20
```

This is a 16 byte hex string (128bit) digest. now the usefulness of a hashing algorithm comes with the fact that if you change the input message, even by a little, the output is vastly different from the original if we instead use a message of "Hello world?" the digest is:

```
48604754B9FED84B3FEEB84C5DC138C0
```

This is a useful property and is used across computing to compare files for equality. Even one single byte of difference in the message will produce a completely different digest as output. As the digest is of a fixed length these can be sent along with every file and each can be calculated at the destination and any incorrect bytes can be safely detected. This is the equivalent of a checksum found on many different bar-codes. Now of course the number of different messages possible is infinite, however given the example of MD5 with its 128bit digest you *only* have $\approx 2^{128} \approx 10^{38}$ possible hashes. This means that there will be some messages that have the same digest. This is a problem, consider you are downloading a new program along with the hash

from a software company, you only want to install the program if you can be sure that the program is exactly the one that was published. If you run a program and it turns out not to be the promised software but instead to be a virus you will be very disappointed. If it was an easy to create two files with the same digest then it could be possible to create a virus program with the same hash as your intended program. When two such messages both have the same digest this is called a collision. In order to have a successful hashing algorithm you must decrease the probability of this happening. The effectiveness of a hashing algorithm is the combination of the possibility of collisions and a quick calculation speed.

1.3 Symmetric key cryptography

As the name suggests symmetric key cryptography is the process of encrypting a message with two symmetric (identical) keys. This encryption should also prevent anyone without a key to do the same. This encryption should then allow the message to be passed through a third party (in most cases the internet) to the intended recipient who has a copy of your key. This type of encryption allows large amounts of data to be securely sent. However one of the main problems with this is that both parties must have the key used to encrypt. This means that they must have a secure way to send the key. And given the fact that they wish to encrypt a file they probably don't have a secure connection between them. One possible solution is that they could both have a common list of keys each with a unique number. when one wishes to send an encrypted file they must only send the unique key number and the encrypted file. They would have to pre generate the keys and send them on a private (secure) network. There are a few different things that must be considered when creating these encryption techniques. The ability to, from an encrypted file, correctly identify the key used to encrypt it which is obviously not a good thing. The ability to brute force the encryption on a file by trying all possible keys. the algorithm can prevent this by ensuring that the process takes a sensible amount of time to run. I.e. too long and the encryption is useless because it has a delay in sending information and too short and its too easy to guess many different keys. The last problem of speed will become apparent later with the section on quantum cryptography.

1.4 Antisymmetric key cryptography

This is similar to the above symmetric key cryptography, however the interesting part about this is in the key pair. When a public key pair is generated one is chosen as the public key and the other as the private key. The public key is put on display by a trusted third party and the private key is saved and kept secure where no one but the creator has access. Like traditional cryptography, both keys can encrypt the message however once a message has been encrypted only the other key can decrypt it. This has two main implications:

- Any file can be securely sent to the (private) key holder by encrypting the file with the public key. This ensures that only the key holder can access the file.
- The key holder 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 properties can be used in order to create a trust relationship between two parties. For example the git server verifies that the commit has not been tampered with by anyone on the network by checking the commit was encrypted with the private key of a user autorised to contribute to the repository. This is all guaranteed because only the owner of the private key can create a signed file. The opposite is also useful. Your bank may publish their public key and with each web page they serve they could include an encrypted hash of the content. you can then verify that the hash is the same as that of the web page and trust that the bank was indeed the creator of the page.

2 Quantum computing

The advent of quantum computing means that the flaws discussed in the processes above could be easily found and the guarantees they give cannot be trusted. Third parties could then break into private conversations and listen in. Files and pages on the internet would not be guaranteed and could not be trusted or verified. This is possible because with classical computation the time required to break these guarantees by brute force is so impossibly large that the in the age of the universe not a single one could have been broken.

However quantum computers offer techniques that were before impossible, and can perform many classical computations many orders of magnitude faster than was before possible.

2.1 Quantum cryptography

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

One such quantum peculiarity is the spin states of photons. The spin of a photon is in one of 4 directions n-s w-e nw-se ne-sw. The quantum nature of the photon means that you cannot measure a photon without disturbing it. this means that if you want to know which direction a photon is spinning then you cant́ then measure it again or pass it along. And you can only measure one set of directions at a time. So you can either choose a n-s or e-w detector and if the photon was in one of the two states then the detector will report the correct direction either n-s or e-w. However if the photon was in one of the other two states nw-se or ne-sw then there is a 50/50 chance that it will report incorrectly either n-s or e-w. So there are two possibilities if you dont́ know which detector to use, you either use the correct detector and get the right result. Or you use the wrong detector and get an incorrect result. however at this point you dont́ know if you are right or wrong.

Now lets use these properties to construct a secure mechanism of sending a string of bytes in such a way that both parties know the exact same string. this can then be used as a traditional key to encrypt the message.

Lets consider those two parties Alice and Bob, Alice wants to communicate a random key to Bob. To do this Alice will encode a string of random data in the spins of photons with different spins and send them to Bob over a glass fibre cable. In order for Bob to decode the photons he will set up a random detector one of the two types ns ew ne-sw nw-se. He will incorrectly measure 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 measurement to Alice. Alice simply replies with the measurements for which Bob used the correct detector. Bob then removes the incorrect measurements and this leaves a list of values that can be converted into a key for standard encryption. Because of the properties of the quantum behaviour of the particles any eavesdropping and measurement of the photons will lead to a message

being unable to be decoded by Bob. This will lead to Alice and Bob knowing that their message was compromised.

3 Conclusion

Cryptography has been around since before the internet and has been an ever evolving science with a basis on mathematical properties and computational complexity. However the quantum revolution has changed this cycle of new algorithms into a more static and proved method. Of course at the moment only the key is transferred over the new principle however in the future the whole process can be secured in this way and then we should be total safe from the prying eyes of others.

The quantum revolution offers many new and different solutions to problems quantum cryptography is one of many different areas of computer science that has been radically changed.