Cryptography

Josh Wainwright

Word Count: 2056

Methods of maintaining security reliably and simply when sending messages has been sought for as long as messages have been sent remotely. In this age of digital communication, email and text messages, this desire for privacy has been more and more difficult to satisfy. A new type of computing brings with it the possibility of a perfectly secure method of transferring messages. Quantum computing still has a long way to go before it common place in homes, but the implications and possible uses of this step forward in computing power are already being employed.

1 Sending a Message

The science of cryptography involves taking a set of data, most commonly a message in some form, but can be any form of digital information, and transforming it in such a way that to anyone but the intended recipient, it is unreadable, and so can be transported safely. The aim is to make breaking the encryption unfeasible rather than impossible.[1] The information is encoded using some pattern or algorithm, called a key or cipher, so that, when this key is passed to the recipient, they can reassemble the message in the original form and so read it.

The first type of computationally driven key was a "symmetric key", so called because the same key is used to both encrypt and decrypt the message, shown in figure 1. This has major flaws, as simply intercepting the transport of the key can allow the whole message which it protects, to be read.

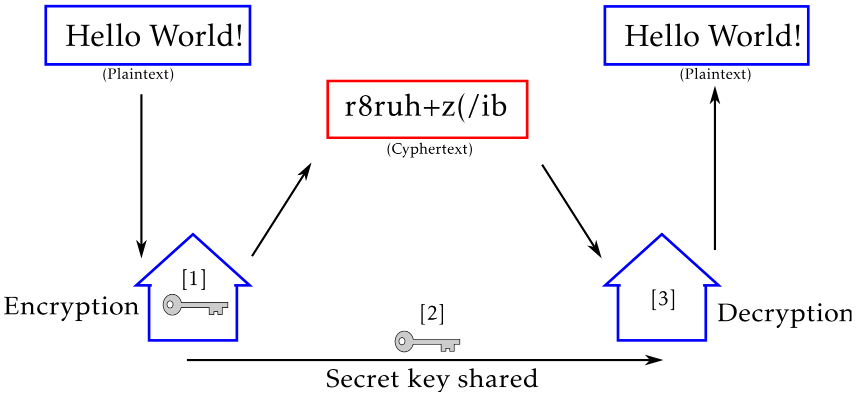

Figure 1: *Symmetric Key Cryptography - the plaintext message to be sent is encoded using a cipher* [1] *(the encoded message is now called cyphertext). The message and this key are then sent to the recipient separately* [2] *so the message can be read* [3]*. The insecurity in this method comes from the transport of the key itself.*

The most commonly used encryption method for use in the public domain now involves using an "asymmetric key" in a technique called public key cryptography. This involves having two keys, one to lock the message and one to unlock it, hence the asymmetric name. The message is locked using the recipient's key that is sent, and so known, publicly, but in such a way that it can only be unlocked again by the private key also owned by the recipient, shown in figure 2. This means that the message can reach the recipient with complete confidentiality, so long as the private key cannot be guessed or calculated from the public key.

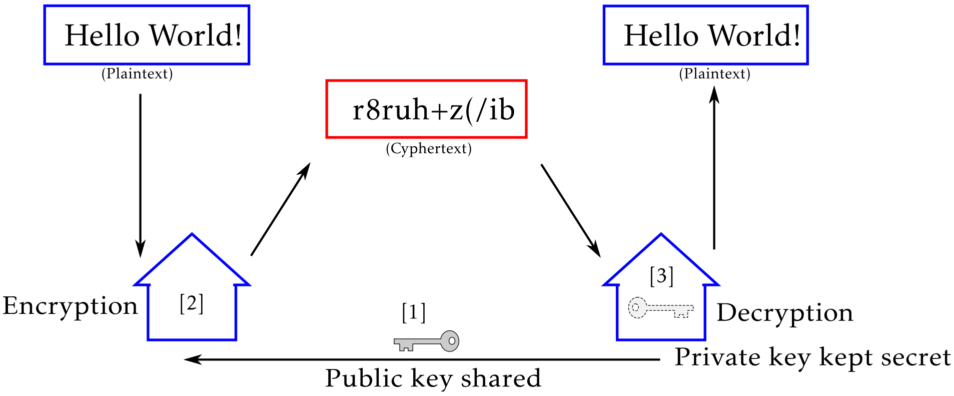

Figure 2: *Asymmetric Key Cryptography - this time the plaintext is encoded* [2] *using the public key sent by the receiver* [1], *then sent as cyphertext to be decrypted with the private key which stays with the receiver at all times* [3].

As technology increases, the ability to calculate the private key is increasing. A great deal of effort is put into developing new algorithms that still retain the necessary properties for an asymmetric key, but are complex enough to make breaking them extremely difficult. Unfortunately, with the advent of ever more complex keys, the computing power needed just to use the private key to open the message increases.

2 Brute Force

It is basically impossible to make anything entirely resistant to attack. In the case of cryptography, an attack constitues the interception of a message or key by any party other than the intended recipient. This breakdown in message security is due to the last resort in breaking cryptographically encoded messages known as a brute force attack. An application of the mathematical technique known as an exhaustive or brute force search, a brute force attack involves sequentially testing every possible combination of keys to break the encoding.

This is generally the last technique to be employed when breaking encryption since a 52 bit encryption key, such as was used for almost all Internet and email security up until the new standard was introduced in 2002,[2] would take about two weeks to break on a fast computer of that time. As the size of the encryption key increases, i.e. the number of digits that would have to be guessed in order to break the code, the time taken to break it also increases. Since the time taken to break the code increases exponentially, an essentially unbreakable encryption system can be built simply by using a large enough key. This has drawbacks however. As the key size increases, possible errors are introduced, the transfer of the key itself can become dangerous and as computing power increases, it is theoretically only a matter of time before the technology will arrive that can break the code.

Another proposed method of making an unbreakable code is to make the message being sent smaller than the key itself, a technique called a "one time pad".[3] This means that there is no way of knowing when the code has been broken as there will be equal probability of any sequence of digits being generated with each possible key attempt. For example if a single byte of text is encoded with a large (e.g. 128 bit) encryption then all hexadecimal bytes, from "00" to "FF", will be equally likely to appear for each attempt at breaking the code. This can be extended to larger messages by changing the key that is used for every section of size equal to the key size.[4]

3 Optical Fibres

Any transmitted message must have an origin and a destination. Even before the issues involved in breaking into the message once it has been acquired are dealt with, the message must be intercepted between these two points so that it can be read.

Most messages that need to be protected by an encryption are digital messages or information. Sending these data involves, at some point in the journey, them travelling through a fibre optic cable. In conventional message transfer systems, this is the most vulnerable part of the journey since simple line tapping techniques can be used to extract information. Indeed, when in an optical fibre, one needs only to introduce a bend to the fibre to allow the information to be split in two and so extract the data. When any information is sent through a fibre optic cable, the information is encoded in bunches of photons that travel in distinct packets delivering their information, either a binary "0" or "1" for each bunch, to the recipient. As the bunches build up, as in figure 3, the message is reassembled.

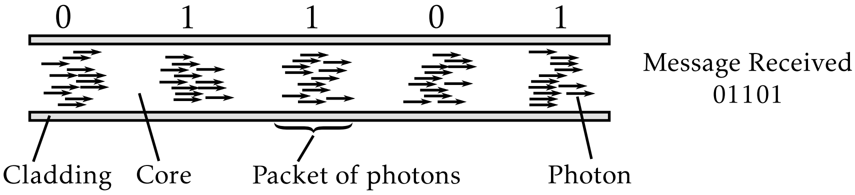

Figure 3: *Fibre optic transfer of a set of information in binary form which reassembles the message as information arrives at the recipient. The information is encoded in the polarization of the photon.*

The issue with fibre optic transfer comes from the number of photons carried in each bunch. In order to ensure that the information can be reliably recreated once it has been delivered, coupled with the methods of creating the photons usually being limited to a large number each time, each bunch contains a very large number of photons. As the photons travel along the fibre optic cable, the phenomena known as total internal reflection means that they will be kept inside the cable, even through bends as demonstrated in figure 4. This is caused by the boundary between the core and the cladding material. When the photons are incident on this boundary with a large angle, i.e. greater than the critical angle, they will be reflected. The critical angle is defined by the difference between the refractive indices of the two materials using their relation given by Snell's law in equation 1,

$$n_i \sin(\theta_i) = n_t \sin(\theta_t). \tag{1}$$

Rearranging Snell's law, gives the the angle of incidence as a function of the two indices and the transmission angle,

$$\theta_i = \sin^{-1}\left(\frac{n_t}{n_i}\sin(\theta_t)\right). \tag{2}$$

The critical angle is defined as the angle at which no light is transmitted from the incident material to the transmission material. The lower limit of this situation is when the light is transmitted at an angle of 90° to the normal, i.e. $\theta_t = 90°$, and $\sin(\theta_t) = 1$. In this case, the critical angle is given by equation 3,

$$\theta_c = \theta_t|_{\theta_i=90°} = \sin^{-1}\left(\frac{n_t}{n_i}\right). \tag{3}$$

This works in principle. However, when the photons travel a great distance, or the path they take is complex, some of the photons will be incident at the boundary with an angle less than

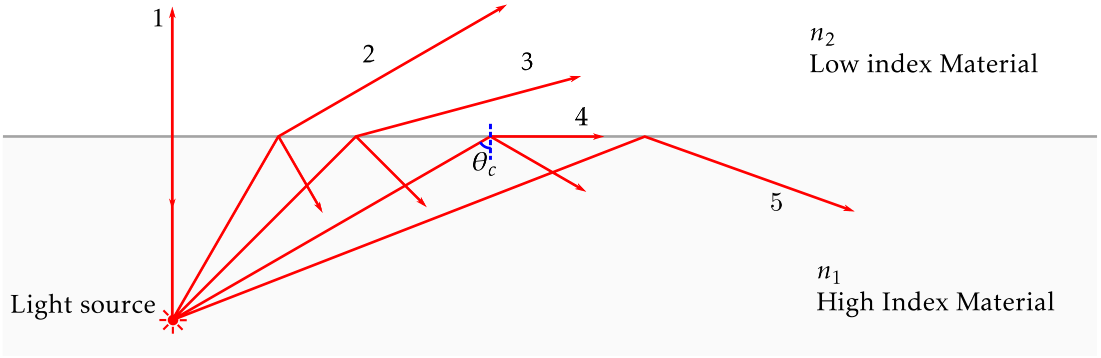

Figure 4: *Most of the photons are maintained within the cable. However, some, that are incident at an angle less than the critical angle, θ_c (equation 3), are lost to the surroundings. Each of the photon paths show an incident angle that increases from 1 to 5. Paths 1 to 3 show how some of the photons can be lost from the core. Path 4 is at the critical angle. The photons in path 5 are all kept within the fibre optic core due to the effect of total internal reflection. This effect requires the difference in refractive index $n_1 > n_2$.*

the critical angle. This will mean that they are transmitted out of the core and lost to the surroundings. In conventional data transfer this is not an issue of great consequence, and is accounted for by the large number of photons in the bunch. It does however present a problem when security is important. The high number of photons means that some can be intercepted by a potential eavesdropper to be analysed, without the recipient knowing the integrity of the message has been compromised.

4 Quantum Cryptography

The latest method developed to combat this sort of breakdown in security involves a change in the way the information is sent through the fibre optic cable. Using modern laser technology, single encoded photons can be produced at high speed on demand. This means that rather than having large bunches of photons, with each photon in a bunch carrying the same information, single photons can be transmitted, one after the other. Several methods of encoding the actual information in the photons have been tried. The first, performed by Bennett and Brassard in 1989,[5] over a distance of 30cm in air, was using the polarisation, for example, a clockwise polarisation would represent a binary "1" and anticlockwise, a "0". The downside of this technique, however, is that transmitting photons along an optical fibre instead of in air can randomise their polarisations. Instead, the phase of the photon is used, which can be measured by the receiver using a configuration of interferometers. Each of these methods involves encoding the message and sending the ciphertext through public channels, then using whatever technique is chosen to send the key. In quantum mechanical cryptography, this is known as practical quantum key distribution, or QKD.

The benefit of using single photons arises from the quantum mechanical properties found only at the very smallest scales of physics. When the large number of photons in the bunches in classical cryptography are used, a few photons can be removed leaving the message largely unchanged. For the single photon system, this is clearly not the case as removing a single photon would alter the message. But the advantages go deeper than this. If an eavesdropper attempts to clone a photon so that it remains in the message but they have a copy, then the laws of quantum mechanics become apparent. Since Heisenberg's Uncertainty Principle states that any measurement on a system must have a corresponding effect on that system, the photon cannot be copied without there being some trace that can be observed when the message arrives at its destination. This means that using this technique, the message can be kept secret, and the presence of any eavesdropper can be detected.

In QKD, the one time pad method is used to increase the security, though this does increase the amount of information that requires transmitting through the optical fibre. For a complete QKD system, the typical bit rates for secure communications are in the range $10-50$kbit/s.

As the technology to break the encryption on data increases, so the methods for encrypting and sending the data must progress. The advances of quantum cryptography represent a large jump forward in the security of digital media, with some suggesting that this offers a 100% secure method of communication. As with every new technology, the accuracy extent of these claims is yet to be substantiated, and it is inevitable that improvements will have to be made. In the mean time, however, every advance made brings us closer to the major goal in current computing research, the fully operational, commercial quantum computer. Will it live up to expectations?

Notes

[1] Algorithms and Combinatorics - Modern Cryptography, Probabilistic Proofs and Pseudo-randomness O. Goldreich pg. 27

[2] Federal Information Processing Standards Publication 197 November 26, 2001 "Announcing the ADVANCED ENCRYPTION STANDARD (AES)"

[3] U.S. Patent 1,310,719 Gilbert S. Vernam, of Brooklyn, New York, assignor to American Telephone and Telegraph Company

[4] Shannon, Claude (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal 28 (4): 656-715.

[5] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental Quantum Cryptography J. Cryptol 5 3-28