Cryptography Primer

Cryptography, in the dictionary, is the art of writing or solving codes. In Wikipedia, it's the practice and study of techniques for secure communication in the presence of third parties called adversaries. I call it sharing a secret. And the perfect, **unbreakable** way to do it was invented over 100 years ago by an engineer named Gilbert Vernam. His code, or cipher, is called the **One Time Pad**, or **OTP**. The reason they use the word *pad* instead of *key* is because of how the OTP works: for every 'letter' of your secret message, you mix it with a 'letter' from a key – you can only use the key 'letter' *one time*, and because your secret could be long, the key was a pad of paper with random 'letters' on it.

That's it: An OTP is an unbreakable cipher, using a key only once, to hide each 'letter' of your message. The reason 'letter' is in quotes, is because nowadays, all of your secrets are electronic messages that use bytes, made up of individual bits, to form the 'letters' – which sometimes are actual alphabetic letters and numbers, but for other things, like a voice over a telephone wire, they are bytes and bits that are transmitted over a communications network using some kind of electronic *protocol*.

These protocols are used in all kinds of electronic networks, from sound to SMS texting to Internet web pages. There are security protocols that perform cryptography used in these different communication protocols: *but none of them use Gilbert's Unbreakable Cipher!* That's because, as you might have guessed, since you can only use a key *one time*, and you and your secret-sharing partner aren't standing right next to each other, *you two need to have pre-shared a whole bunch of OTP's – one time keys – one for each and every message you each send! That's a lot of keys!*

You might remember the old spy movies, where there was a guy dressed in black, with an attaché case handcuffed to his wrist going to the embassy: That case was full of all the next month's OTPs! Now since we can't all have spy's running all over the world, there's a Big Problem using the perfect, unbreakable OTP: The **Key Distribution Problem:** We all need one time keys, for each of our intended secret message recipients, for every single message! This *seems to be* an insurmountable, unsolvable problem, doesn't it?

In the 1970's, some very smart people discovered a way, based on **mathematic theory**, to attempt to solve the problem – it's called **Public Key Cryptography** – and it is the basis of systems called a **Public Key Infrastructure**, or PKI – these are used in those security protocols. Somehow, over the last 50 years, these PKI's have been presented as *solving, or even eliminating*, the distribution problem. Unfortunately, there is a simple way to know whether or not they actually did: *Are you sharing your secrets electronically using that original, unbreakable OTP cipher inside a PKI protocol*? **No.** The answer tells you that the problem wasn't solved by these systems; the methods and underlying ciphers that are used have several problems, like performance and efficiency – but the real tragedy is that cryptography lost *unbreakable!*

QwyitTalk™ *actually does solve the key distribution problem* – and you know it because it *does use the OTP cipher as the unbreakable code* that keeps your messages secure. And QwyitTalk™ retained the best property of the PKI systems: you, and all of your secret messaging partners, only need one key to start all of your OTP unbreakable secret sharing. That original, secret key *makes a new OTP key for every letter of your messages* by using **mathematic fact,** *not theory* – so not only is the underlying cipher unbreakable, the entire cryptosystem is too! QwyitTalk™ removed all of those other PKI problems, allowing the future of all your messages – including in as-yet-imagined ways – to be unbreakably private and secure.

Cryptography evolved up to 100 years ago with the introduction of the final cipher: unbreakable OTP. Today, QwyitTalk™ has solved the last remaining engineering problem of how to share and create all of the necessary OTP keys, making a complete unbreakable cryptosystem. Now all that remains to be done is for us to use it!