Qwyit® Time

This document details how *QCy*™ is the only existing viable Perfectly Secret (Unbreakable) Post-Quantum Cryptography (PQC). For this document, as well as in general discussions/communications, *Qwyit*® refers to the Company, *Qwyit*™ refers to the complete Authentication and Data Encryption protocol and *QCy*™ refers to the encryption cipher. Definitions and operation of all of our security technology can be found in their current *Reference Guides* available from Qwyit®; go to www.qwyit.com.

Introduction

Solving a cryptographic encryption cipher has two aspects that directly affect discovering the original plaintext message (e.g., *Breaking* the algorithm):

1. *Method*
   a. The process/algorithm used to encrypt

2. *Time*
   a. How long it takes to operate the 'decrypt-to-the-correct-plaintext-without-the-key' process

These, in turn, have pertinent elements:

- How *strong* is the *Method*?
- What *resources* are available when spending *Time*?

Therefore:

A *Break* occurs when one has spent enough time filled with resources to overcome the method's strength using some process. *Break* = $\mathit{Method}_{\mathit{Strength}}$ overcome in $\mathit{Time}_{\mathit{Resources}}$

Discussion

Strength

Cryptography uses all kinds of definitions of cryptographic strength – these are overly complex such that only cryptographers (security experts) understand them. Let's use plain English descriptions for general comprehension. After all, *routine use of digital security is best practiced and provided when the 'average user' fully understands how and why it actually works.*

Shannon's Communication Theory of Secrecy Systems provides the *strength* scale: Theoretical and Practical. He breaks these down into their results:

- Theoretical Security
  - Perfect Secrecy – Mathematically provably Unbreakable
    - There will never be a *Break,* such that *Time* is forever
    - An example *Method* of this is the One Time Pad (OTP) [1]

[1] While Quantum Cryptography appears to be theoretically unbreakable, the limitations and binary PS existence, render it questionable

  - Strongly Ideal System Perfect Secrecy – Unbreakable; difficult to prove mathematically, yet the Method delivers the same result: multiple different plaintexts produce identical ciphertext
    - There will never be a *Break,* such that *Time* is forever
    - The only existing *Method* of this is *QCy*™

- Practical Security
  - All single-result ciphers: every different plaintext produces different ciphertext
    - There will always be a *Break*, given enough *Time*
    - This is every cipher created other than Perfect Secrecy (OTP, *QCy*™)

<u>Resources</u>

Resources can generally be summarized into the 'current computing capability'; which is used to power the *Time (T)* process to break an algorithm. An algorithm is considered time/resource broken in several different definitions: 'solution found prior to brute force time', 'solution found in less than the design criteria time'. Etc.

The meaningful definition is that the *Break* can be performed in *Real Time*. In math/computing, this is called Polynomial Time; in real life, for average users, this is called *Now.* 'Now' means that in a time in which the protection should be valid, it is not – it can be compromised/broken yielding loss to the user. This may be instantly, daily, monthly, yearly – realistically:

A *Break* occurs when the current computing capability can decipher an algorithm's ciphertext into plaintext without any secret knowledge at *Time Now.*

This means that when *Time* was:

- Ancient – before computing
- Analog – early machine computation available
- Digital – Now, 2023

…Practical Security was sufficient. It is cryptographically acceptable to use today's *Methods*, because the *resources* available are unable to result in *Breaks Now. Time* is still a singular security protection.

But when *Time* becomes:

- Quantum – soon…
- Artificial – coming…
- Forever *NOW* – eventually!

…Practical Security is impractical and useless, *Breaks* occur *Now.* One must use Theoretical Security*.*

Conclusions

In order to provide actual *Time Independent* Theoretical Security in Post-Quantum Cryptography, such that encryption has any value, only OTPs and *QCy*™ are available. Using these is the only choice; the only *Method* where, no matter the resources and escalating computing power, there is never a *Break.* Since OTPs have key management practically issues, there's only one remaining cryptographically forever Perfectly Secret *Method*: *QCy*™*.* Start using it *Now.* It's Qwyit® Time.