**JANGLE: LINGUAL BASED ENCRYPTION**

_Jangle is a new kind of encryption tool based on language instead of mathematics._

**PROBLEM**

With current information security technology, business losses due to cybercrime are projected to top $2 trillion in 2019. At the core of current information security are two components: math-based cryptography and a well-developed sense of paranoia. Math-based cryptography has been the go-to tool for encrypting messages for much, if not all, of human history. However, the advent of computer technology has given rise to an encryption “arms race” in which adversaries compete to build the fastest computer and hence possess the most powerful encryption/decryption capability.

**SOLUTION**

A novel approach to encryption is lingual transformation (LT). Just as humans use slang influenced from their current social environment to communicate covertly without resorting to mathematical transformations, so too could we program computers to generate ciphertext by representing transmissions in “slang” arising from the current transmission environment.

This means computers could rapidly and continuously create new, throwaway languages for one-time use between two nodes on a network, based on the context of their own previous exchanges. There would be no need for (quasi-) random key generation, nor any math to perform, so the speed at which an attacker’s computer can execute mathematical operations would be irrelevant. The idea of computers creating and communicating in their own slang, as humans do, is conceptually appealing because language is humans’ default thought mechanism, unlike mathematics, which is the default strength of computers.

The one-time-use “languages” generated by communicating nodes may or may not necessarily resemble human language; they need not even use words in the everyday sense. Referring to the context that only they (the two nodes) share, they need only agree on which symbol(s) will convey which meaning.

**BENEFITS**

This technology would reduce business losses due to cybercrime by providing more secure Virtual Private Networks (VPN). Data communication that cannot be forced mathematically and is not vulnerable to other forms of attack (like replay and man-in-the-middle) is a vast improvement of current technology.

**APPLICATIONS**

Jangle can be applied to VPNs in public, private, business, personal, institutional and governmental arenas.