Cryptology beyond Shannon's Information Theory: Preparing for When the 'Enemy Knows the System'

With Technical Focus on

Number Field Sieve

Cryptanalysis Algorithms for Most Efficient Prime Factorization on Composites

Yogesh Malhotra, PhD
www.yogeshmalhotra.com
Griffiss Cyberspace, Global Risk Management Network, LLC
www.griffisscyberspace.org, www.finrm.org

May 03, 2013

"A cryptosystem should be secure even if the attacker knows all details about the system, ~~with the exception of~~ including the secret key."

- Yogesh Malhotra's reformulation of Kerckhoffs's principle, 2013

"The enemy knows the system*, but you 'know' better*."

- Yogesh Malhotra's reformulation of Shannon's maxim, 2013

Abstract

"A cryptosystem should be secure even if the attacker knows all details about the system, ~~with the exception of~~ including the secret key."

- Yogesh Malhotra’s reformulation of Kerckhoffs's principle, 2013

"The enemy knows the system*, but you ‘know’ better*."

- Yogesh Malhotra’s reformulation of Shannon’s maxim, 2013

The problem is introduced as creation of encryption algorithms whose *cracking* is computationally infeasible. Hegelian dialectic questioning that premise is posed by invoking Poe asking if it is even possible for human ingenuity to ‘concoct a cipher’ which human ingenuity cannot resolve. Symmetric and public key cryptography as well as various RSA benchmarks are reviewed to develop a *sense* of the encryption vulnerability trend. Apparent *overconfidence* of expert scientist Rivest in his RSA encryption is introduced as what he later called ‘our *infamous* “40 quadrillion years”’ challenge.[1] Recognizing that the ‘40 quadrillion years’ challenge became unraveled in less than a minuscule of tiniest fraction of order ~ 10^{-15} of estimated time to failure is the backdrop of the timeline of RSA failures depicting strong encryption vulnerability trend. Next RSA benchmark on cusp of being cracked – *unless it has already been cracked in private* – is the global encryption standard RSA-1024 in worldwide use for the most critical national, economic and industrial activities. Factoring algorithms, the *devil’s advocate* to cryptologists’ claim of computational infeasibility of encryption failures are introduced with discussion of general and special purpose factoring algorithms. Central technical focus is on Number Field Sieve (NFS), *most potent of all factoring known algorithms* used for recent strongest attacks. 5-phase operation of NFS is discussed with specific focus on: polynomial selection, finding factor bases, sieving for optimal congruent relations, solving linear equations with matrix, and computing square roots in number fields.

Then my investigation returns to the original question: What if Poe’s foresight about human cryptologist’s ingenuity not being able to outsmart human cryptanalyst’s ingenuity was not far from reality? Increasingly devastating real world encryption failures are reviewed lending credence to Poe’s thesis. Parallels between Poe’s insight and Claude Shannon’s *maxim* and Kerckhoffs's principle are clarified. By adapting both to *bridge information theoretic information processing* and my work on *human sense making* (Malhotra 2001) I introduce the *sketch* of a new cryptology principle: *Malhotra’s principle of no secret keys*. The proposed sketch develops upon my 20-yr information and communication systems research which also included focus on issues such as competitive intelligence, misinformation and disinformation. It further advances beyond my original communication with John Holland, the inventor of genetic algorithms in 1995. Based on Holland’s observation that Shannon’s notion of *information* in *information theory* missed critical human aspects of *meaning*, *sense making*, and *knowing*, my research developed a widely accepted *knowledge management* framework applied by global organizations such as NASA, US AFRL, US Army, US Navy, and US Air Force. The proposed principles based on that framework aim to complement Shannon’s information theory originally designed for *controlling machines* based on my research on the psychology of *information, meaning, sense making,* and *knowing*. What *having* and *knowing* mean in the *human behavior framework* can fundamentally advance notions such as information theory based two factor authentication by fundamentally rethinking and reformulating very basic ideas such as: something that you *have* and something that you *know*.

[1] Rivset, Ronald R. The Early Days of RSA – History and Lessons, ACM Turing Award Lecture.