Contribution ID : **27** Type : **not specified**

The Quest for the Missing Keytags

Friday, 1 April 2016 11:30 (30)

In an effort to create all possible 64K keytags for a DNSSEC signing key, an anomaly surfaced that caused 75% of the possible keytags to never appear.

This effort to generate certain cryptographic keys became an adventure in itself that included beautiful discrete math, flawed functions, carefully crafted primes, multiple cryptographic libraries, and some brilliant people.

The result of this effort shows that using an ancient checksum function to identify cryptographic keys is not optimal.

Summary

The presentation will go through the quest of uncovering the anomaly that caused the limitation in keytags generation.

Primary author(s) : ARENDS, Roy (ICANN)

Presenter(s) : ARENDS, Roy (ICANN)

Session Classification : Public Workshop: Research

Track Classification : Public Workshop