Encryption and Cryptographic Hashing Standards

Minimum Encryption Requirements

In any situation where the University requires that cryptography be employed, the following are the minimum standards of such encryption or cryptographic hashing:

- industry standard cryptographic algorithms that have not been shown to be vulnerable "in the real world", e.g., the SHA-1 standard has theoretical vulnerabilities but no collisions have yet been found. SHA-2 or SHA-3 would be preferred as a result, not required at this time, but possibly required in the near future.
- implemented through widely used and tested libraries
- utilizing at least 128 bits of complexity for symmetric encryption
- 2048 bits for asymmetric key based encryption.

Elevated Requirements

In certain cases due legal or regulatory requirements or based on risk assessments, IT Services may require that specific cryptographic algorithms be employed or excluded depending upon the particular IT resource being protected.

Implementation

Since previous versions of this standard allowed for use of 1024 bit keys for asymmetric encryption, systems currently using 1024 bit keys may continue to operate with existing keys until such time as the keys need to be refreshed or re-implemented. At that time, system owners or administrators should implement 2048 bit keys. However, in no case should 1024 bit keys be employed after January 1, 2015.

Examples

The following are a few examples of how encryption can be used to meet the University requirements. This is not an exhaustive list as there are many acceptable ways to meet the encryption requirements.

- ssh Version 2 (Version 1 does not meet the requirements as there are demonstrated vulnerabilities in the protocol) for communication between two machines across a network
- the University of Chicago Virtual Private Network (VPN) for working with data on University servers while at home or traveling
- PGP, using a key of a minimum of 2048 bits, to encrypt data either being stored on a remote server or being sent via email