In light of the widespread deprecation of SHA1 due to collision risk it poses, should Ruby still expose it without a warning within Digest::SHA1?

FIPS PUB 180-1 which is referenced by the Digest::SHA1 documentation was withdraw on August 01, 2002, superseded by FIPS 180-2 (which introduced SHA-256, SHA-384, and SHA-512), and later withdrawn and superseded multiple times until FIPS 180-4 which recommends SHA3.

SHA3 isn't currently supported by the Digest class although there exists Ruby gem implementations:

- [https://github.com/johanns/sha3](https://github.com/johanns/sha3)
- [https://github.com/phusion/digest-sha3-ruby](https://github.com/phusion/digest-sha3-ruby)

References:

- [https://mailarchive.ietf.org/arch/msg/openpgp/Rp-inhYKT8A9H5E34iLTc9i0gc/](https://mailarchive.ietf.org/arch/msg/openpgp/Rp-inhYKT8A9H5E34iLTc9i0gc/)

Quoting from NIST's piece on research regarding SHA1 collisions:

NIST deprecated the use of SHA-1 in 2011 and disallowed its use for digital signatures at the end of 2013, based on both the Wang, et. al, attack and the potential for brute-force attack. To ensure that practitioners have secure and efficient hash algorithms to provide long-term security, NIST organized an international competition to select a new hash algorithm standard, SHA-3, which is specified in FIPS 202.

My recommendation would be to print a deprecation warning when Digest::SHA1 is used to alert Ruby users that they should perhaps upgrade to a safer standard. SHA3 should perhaps be supported by Digest as well.

History

#1 - 10/24/2020 05:34 AM - jeremyevans0 (Jeremy Evans)

Note that we don't currently even deprecate MD5, and if we were going to deprecate SHA1 due to security issues, we should deprecate MD5 first since it's even worse. I think we should strongly discourage the use of MD5 and SHA1 in the Digest documentation, but a deprecation warning on usage is going too far. Not all usage of SHA1 is vulnerable (e.g. HMAC-SHA1), and SHA1 is still in wide enough usage (e.g. git) that a deprecation warning on usage is going to be annoying. These days, the majority of usage of SHA1 in Ruby is not when you are choosing the algorithm, but when you are forced to use the algorithm in order to interact with other software and usage is unavoidable. I think we shouldn't deprecate Digest::SHA1 (or Digest::MD5) until we plan on removing it the next Ruby release.

I'm in favor of SHA3 support being added to Digest, but please submit a separate ticket for that.

#2 - 10/26/2020 01:12 AM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Third Party's Issue

Digest is now a separate project. [https://github.com/ruby/digest](https://github.com/ruby/digest)

P.S. I want "2nd party's issue" status. ruby/digets is not a 3rd party.