Reviving draft-irtf-cfrg-webcrypto-algorithms?

Updating the draft to reflect current algorithms and sensibilities

Current status of draft-irtf-cfrg-webcrypto-algorithms

Network Working Group — H. Halpin, Ed. W3C/MIT
Internet-Draft — G. Steel Cryptosense/INRIA
Intended status: Informational — November 20, 2015
Expires: May 23, 2016

Security Guidelines for Cryptographic Algorithms in the W3C Web Cryptography API
draft-irtf-cfrg-webcrypto-algorithms-00

Algorithm/Mode	OK Legacy	OK Future	Note
RSAES-PKCS1-v1_5	YES	NO	
RSA-OAEP	YES	YES	
RSASSA-PKCS1-v1_5	YES	NO	No public security proof
RSA-PSS	YES	YES	
ECDSA	YES	YES	Controversy
ECDH	YES	YES	Controvery
AES-CBC	YES	YES	NB not CCA secure
AES-CFB	YES	YES	NB not CCA secure
AES-CTR	YES	YES	NB not CCA secure
AES-GCM	YES	YES	
AES-CMAC	YES	YES	
AES-KW	YES	NO	No public security proof
HMAC	YES	YES	
DH	YES	YES	Only using strong parameters
SHA-1	YES	NO	Known weaknesses (see text)
SHA-256	YES	YES	
SHA-384	YES	YES	
SHA-512	YES	YES	
CONCAT	YES	YES	
HKDF-CTR	YES	YES	
PBKDF2	YES	NO	Known weaknesses (see text))

Algorithm/Mode	OK Legacy	OK Future	Note
~~RSAES-PKCS1-v1_5~~	~~YES~~	~~NO~~	
RSA-OAEP	YES	YES	
RSASSA-PKCS1-v1_5	YES	NO	No public security proof
RSA-PSS	YES	YES	
ECDSA	YES	YES	Controversy
ECDH	YES	YES	Controvery
AES-CBC	YES	YES	NB not CCA secure
~~AES-CFB~~	~~YES~~	~~YES~~	~~NB not CCA secure~~
AES-CTR	YES	YES	NB not CCA secure
AES-GCM	YES	YES	
~~AES-CMAC~~	~~YES~~	~~YES~~	
AES-KW	YES	NO	No public security proof
HMAC	YES	YES	
~~DH~~	~~YES~~	~~YES~~	~~Only using strong parameters~~
SHA-1	YES	NO	Known weaknesses (see text)
SHA-256	YES	YES	
SHA-384	YES	YES	
SHA-512	YES	YES	
~~CONCAT~~	~~YES~~	~~YES~~	
HKDF~~-CTR~~	YES	YES	
PBKDF2	YES	NO	Known weaknesses (see text))

Algorithm/Mode	OK Legacy	OK Future	Note
~~RSAES-PKCS1-v1_5~~	~~YES~~	~~NO~~	
RSA-OAEP	YES	YES	
RSASSA-PKCS1-v1_5	YES	NO	No public security proof
RSA-PSS	YES	YES	
ECDSA	YES	YES	Controversy
ECDH	YES	YES	Controvery
AES-CBC	YES	~~YES~~ No?	NB not CCA secure
~~AES-CFB~~	~~YES~~	~~YES~~	~~NB not CCA secure~~
AES-CTR	YES	~~YES~~ No?	NB not CCA secure
AES-GCM	YES	YES	
~~AES-CMAC~~	~~YES~~	~~YES~~	
AES-KW	YES	NO	No public security proof
HMAC	YES	YES	
~~DH~~	~~YES~~	~~YES~~	~~Only using strong parameters~~
SHA-1	YES	NO	Known weaknesses (see text)
SHA-256	YES	YES	
SHA-384	YES	YES	
SHA-512	YES	YES	
~~CONCAT~~	~~YES~~	~~YES~~	
HKDF~~-CTR~~	YES	YES	
PBKDF2	YES	NO	Known weaknesses (see text))

Questions

- Agree that this work is (still) worthwhile?
- Want to help? :)

Thoughts? Questions?