Web Cryptography API Cheat Sheet

SubtleCrypto Interface

```
encrypt(AlgorithmIdentifier algorithm,
      CryptoKey key,
      BufferSource data);

decrypt(AlgorithmIdentifier algorithm,
      CryptoKey key,
      BufferSource data);

sign(AlgorithmIdentifier algorithm,
      CryptoKey key,
      BufferSource data);

verify(AlgorithmIdentifier algorithm,
      CryptoKey key,
      BufferSource signature,
      BufferSource data);

digest(AlgorithmIdentifier algorithm,
      BufferSource data);

generateKey(AlgorithmIdentifier algorithm,
      boolean extractable,
      sequence<KeyUsage> keyUsages );
```

```
deriveKey(AlgorithmIdentifier algorithm,
      CryptoKey baseKey,
      AlgorithmIdentifier derivedKeyType,
      boolean extractable,
      sequence<KeyUsage> keyUsages );

deriveBits(AlgorithmIdentifier algorithm,
      CryptoKey baseKey,
      unsigned long length);

  importKey(KeyFormat format,
      (BufferSource or JsonWebKey) keyData,
      AlgorithmIdentifier algorithm,
      boolean extractable,
      sequence<KeyUsage> keyUsages );

exportKey(KeyFormat format, CryptoKey key);

wrapKey(KeyFormat format,
      CryptoKey key,
      CryptoKey wrappingKey,
      AlgorithmIdentifier wrapAlgorithm);

unwrapKey(KeyFormat format,
      BufferSource wrappedKey,
      CryptoKey unwrappingKey,
      AlgorithmIdentifier unwrapAlgorithm,
      AlgorithmIdentifier unwrappedKeyAlgorithm,
      boolean extractable,
      sequence<KeyUsage> keyUsages );
```

From W3C Candidate Recommendation at https://www.w3.org/TR/WebCryptoAPI/

Web Cryptography API Cheat Sheet

Algorithms and Operations

Encryption

Symmetric: AES-CTR, AES-CBC, AES-GCM, AES-CFB, AES-KW (no general encrypt/decrypt)
Asymmetric: RSA-OAEP
Methods: encrypt, decrypt, generateKey, importKey, exportKey, wrapKey, unwrapKey

Digital Signature

Symmetric: AES-CMAC, HMAC
Asymmetric: RSA-PKCS1-v1_5, RSA-PSS, ECDSA
Methods: sign, verify, generateKey, importKey, exportKey

Message Digest

Algorithms: SHA-1, SHA-256, SHA-384, SHA-512
Methods: digest

Others

Key exchange: ECDH, DH
Methods: generateKey, deriveKey, deriveBits, importKey, exportKey

Key derivation: CONCAT, HKDF-CTR, PBKDF2
Methods: deriveKey, deriveBits, importKey, generateKey (PBKDF2 only)

Algorithm Identifier Examples

generateKey

name: AES-CBC
length: 256

name: RSASSA-PKCS1-v1_5
modulusLength: 2048
publicExponent: new Uint8Array([1,0,1])
hash: SHA-256

name: RSA-OAEP
modulusLength: 2048
publicExponent: new Uint8Array([1,0,1])
hash: SHA-256

name: PBKDF2

importKey

name: AES-CBC

name: RSASSA-PKCS1-v1_5
hash: SHA-256

name: RSA-OEAP
hash: SHA-256

name: PBKDF2

From W3C Candidate Recommendation at https://www.w3.org/TR/WebCryptoAPI/