


01-Web_Cryptography_API

Introduction

This note gather information obtained during my discovery of the **Web Cryptography API**.

Security attention points

All element marked with  are points that must taken in account from a security point of view.

Misc

- Table were generated with [this tool](#).

Study roadmap

- ☐ Search and explore documentation and tutorials.
- ☐ Implement the labs.
- ☐ Create a XLM blog post about all this study.

Sources

- [RFC](#)
- [MDN DOCS](#)
- [MDN SAMPLES](#)
- [CHROMIUM](#)

Note for the blog post

The blog post will have the following section:

1. What is the Web Cryptography API?
2. Browser support level?
3. Why it is interesting to use it (pro/con)?
4. Global overview of its capabilities

For the point 4:

Demonstration of usage for the different kind of crypto operations:

- Hash

- HMAC
- Signature
- Key handling
- Security random number generation (PRNG)
- Symetric encryption
- Asymetric encryption

If possible for each crypto operation compare it [CryptoJS](#) with the same context: The risk it t cause a debate/drama...so let's see during the lab/research...

Research

What is the Web Cryptography API?

Information below are taken from the RFC.

JavaScript API for performing basic cryptographic operations in web applications, such as hashing, signature generation and verification, and encryption and decryption.

Additionally, it describes an API for applications to generate and/or manage the keying material necessary to perform these operations.

Cryptographic transformations are exposed via the `SubtleCrypto` interface, which defines a set of methods for performing common cryptographic operations.

This specification does not dictate a mandatory set of algorithms that MUST be implemented (see the reason [here](#)) however it provides descriptions for a variety of algorithms that authors may wish to use and that User Agents may choose to implement.

This API does not deal with or address the discovery of cryptographic modules (see the reason [here](#)).

This specification does not define any specific mechanisms for the storage of cryptographic keys:

By default, unless specific effort is taken by the author to persist keys, such as through the use of the Indexed Database API, keys created with this API will only be valid for the duration of the current page (e.g. until a navigation event). Authors that wish to use the same key across different pages or multiple browsing sessions must employ existing web storage technologies

The only requirement for the API is that key material is not exposed to script, except through the use of the `exportKey` and `wrapKey` operations.

⚠ In particular, the API does not guarantee that the underlying cryptographic key material will not be persisted to disk, possibly unencrypted, nor that it will be inaccessible to users or other applications running with the same privileges as the User Agent.

⚠ Any application or user that has access to the device storage may be able to recover the key material, even through scripts may be prohibited.

⚠ This specification places no normative requirements on how implementations handle key material once all references to it go away. That is, conforming user agents are not required to zeroize key material, and it may still be accessible on device storage or device memory, even after all references to the CryptoKey have gone away.

⚠ Developers making use of the `SubtleCrypto` interface are expected to be aware of the security concerns associated with both the design and implementation of the various algorithms provided.

⚠ This specification includes several algorithms which, in their default usage, can result in cryptographic vulnerabilities. While these concerns may be mitigated, such as through the combination and composition with additional algorithms provided by this specification, authors should proceed with caution and review the relevant cryptographic literature before using a given algorithm: See [here](#).

⚠ [Security considerations](#).

Supported operations, see [here](#) and [here](#) :

- Get random bytes
- Encrypt / Decrypt using symmetric/asymmetric algorithm/key
- Sign and verify signature using symmetric/asymmetric algorithm/key
- Hash
- Generate symmetric/asymmetric key
- Derive key symmetric/asymmetric key
- Import/export symmetric/asymmetric key
- wrap/unwrap symmetric/asymmetric key (???)

Supported key format, see [here](#) :

- **raw**: An unformatted sequence of bytes. Intended for secret keys.
- **pcks8**: The DER encoding of the `PrivateKeyInfo` structure.
- **spki**: The DER encoding of the `SubjectPublicKeyInfo` structure.
- **jwk**: The key is a [JsonWebKey dictionary](#) encoded as a JavaScript object.

Browser support level?

Support on June 2021:

Source: <https://caniuse.com/cryptography>.

Web Cryptography REC

JavaScript API for performing basic cryptographic operations in web applications

Usage
% of all users
Global
96.13% + 0.85% = 96.98%
unprefixed: 95.48%
Luxembourg
98% + 0.66% = 98.66%
unprefixed: 97.17%

Current aligned
Usage relative
Date relative
Filtered
All

IE	Edge *	Firefox	Chrome	Safari	Opera	Safari on iOS *	Opera Mini *	Android Browser *	Opera Mobile *	Chrome for Android	Firefox for Android	UC Browser for Android	Samsung Internet	QQ Browser	Baidu Browser	KaiOS Browser
		2-31		3.1-7		3.2-7.1										
	12-18	32-33	4-36	7.1-10.1	10-23	8-10.3										
6-10	79-90	34-88	37-90	11-14	24-75	11-14.4		2.1-4.4.4	12-12.1				4-13.0			
11	91	89	91	14.1	76	14.6	all	91	62	91	89	12.12	14.0	10.4	7.12	2.5
		90-91	92-94	TP												

Notes
Test on a real browser
Known issues (0)
Resources (13)
Feedback

Many browsers support the `crypto.getRandomValues()` method, but not actual cryptography functionality under `crypto.subtle`.

- Support in IE11 is based on an older version of the specification.
- Support in Safari before version 11 was using the `crypto.webkitSubtle` prefix.
- In Edge 12-18, Web Crypto was not supported in Web Workers and Service Workers.




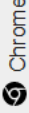

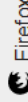
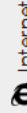

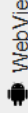
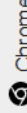
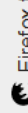


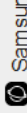

IE	Edge *	Firefox	Chrome	Safari	Safari on iOS *	Opera Mini *	Chrome for Android	UC Browser for Android	Samsung Internet
			89		13.7				
	90	88	90	14	14.4				
11	91	89	91	14.1	14.6	all	91	12.12	14.0
		90	92	TP					
		91	93						
			94						


Source: https://developer.mozilla.org/en-US/docs/Web/API/Web_Crypto_API#browser_compatibility.

Browser compatibility


Crypto


[Report problems with this compatibility data on GitHub](#)

													
	 Chrome	 Edge	 Firefox	 Internet Explorer	 Opera	 Safari	 WebView Android	 Chrome Android	 Firefox for Android	 Opera Android	 Safari on iOS	 Samsung Internet	 Node.js
Crypto	11	12	26	11	15	6.1	37	18	26	14	6.1	1.0	15.0.0 ★ ▼
getRandomValues()	11	12	26	11	15	6.1	37	18	26	14	6.1	1.0	15.0.0
subtle ⚠	37	12	34	11	24	11 ▼	37	37	34	24	11 ▼	3.0	15.0.0
Secure context required	60	79	75	No	47	No	60	60	No	47	No	8.0	?

 Full support

 Partial support

 No support

 Compatibility unknown

Why it is interesting to use it (pro/con)?

The list below present some pros and cons of the using this API.

Pros:

- Ensure that implementation of the algorithms is done by crypto specialists.
- Ensure that security issues on implementation of the algorithms are automatically patched during the browser update process.
- Ensure that the maintenance/update of the API/implementation of the algorithms is done by the browser provider (no abrupt stop of the support).
- Provide, in theory, a "portability" across all browsers supporting the API.

Cons:

- As patching of security issues on implementation of the algorithms is handled by browsers so user must upgrade it browsers itself (warning is possible using JS with browser version info).
- The API support vulnerable algorithms so care must be taken on the algorithms used.
- Security of the key storage is not covered by the API so it must be managed by the app.

- The API RFC places no normative requirements on how implementations handle key material once all references to it go away so exposure of the key is possible in case of memory handling issue.
- As the API provide low level operations, it's up to the developer to ensure a correct usage of the target algorithm according to its specificities (ex: in AES-GCM, requirement of a unique NONCE for each encryption operation).

💡 Even if cons exists, usage of this API is desirable over custom JS libraries if only for the fact it ensure that implementation of the crypto algorithm is performed by specialist in the domain as well the consistent process of patchning provided by the browser. Indeed, most of modern browsers like Firefox, Chrome, Opera and Edge provide auto-update process.

Global overview of its capabilities

📝 Base references used in all code snippets:

```
//See https://developer.mozilla.org/en-US/docs/Web/API/Window/crypto
const CRYPTO_OBJ = window.crypto;
//See https://developer.mozilla.org/en-US/docs/Web/API/TextEncoder
const TEXT_ENCODER = new TextEncoder("utf8");
//See https://developer.mozilla.org/en-US/docs/Web/API/TextDecoder
const TEXT_DECODER = new TextDecoder("utf8");
```

📝 Conversion to HEX function used in some code snippets ([credits](#)):

```
//Credits: https://stackoverflow.com/a/40031979/451455
function toHex(buffer) {
    return [...new Uint8Array(buffer)]
        .map(x => x.toString(16).padStart(2, "0"))
        .join("");
}
```

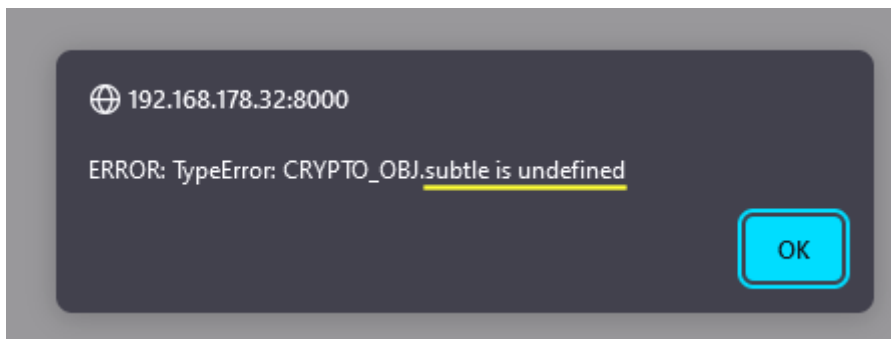
📝 Reference to **Secure Context** means, to simplify, that the protocol used is HTTPS:

SubtleCrypto

🔒 Secure context

This feature is available only in [secure contexts](#) (HTTPS), in some or all [supporting browsers](#).

The following error is raised when the HTTP protocol (non secure context) is used but it is not supported due to the requirement of a **Secure Context** (`subtle` attribute member of the `crypto` object is not defined):



Random values generation

Source: <https://developer.mozilla.org/en-US/docs/Web/API/Crypto/getRandomValues>

⚠ Don't use `getRandomValues()` to generate encryption keys. Instead, use the [generateKey\(\)](#) method. There are a few reasons for this; for example, `getRandomValues()` **is not guaranteed to be running in a secure context**.

⚠ See value limitation [here](#).

Can be used in the context of the following protocols:

- HTTP: ✓
- HTTPS: ✓

Code snippet:

```
function performRandomValuesGeneration(wantedLength) {  
    let buffer = new Int32Array(wantedLength);  
    cryptoObj.getRandomValues(buffer);  
    return toHex(buffer);  
}
```

Hashing

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/digest>

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

```
async function performSha512Hash(sourceData) {  
    let dataEncoded = TEXT_ENCODER.encode(sourceData);  
    let hashBytes = await CRYPTO_OBJ.subtle.digest("SHA-512",  
dataEncoded);  
    return toHex(hashBytes);  
}
```

Symmetric key handling

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/generateKey>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/AesKeyGenParams>

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

```
async function
performSymmetricKeyGenerationForEncryptionDecryptionUsageWithAESGCM() {
    //Generate a 256 bits key for AES-GCM symmetric encryption algorithm
    //See https://developer.mozilla.org/en-US/docs/Web/API/AesKeyGenParams
    let aesKeyGenParams = {
        name: "AES-GCM",
        length: 256
    };
    let keyUsages = ["encrypt", "decrypt"];
    //See https://developer.mozilla.org/en-
US/docs/Web/API/SubtleCrypto/generateKey
    let cryptoKey = await CRYPTO_OBJ.subtle.generateKey(aesKeyGenParams,
true, keyUsages);
    return cryptoKey;
}
```

Symmetric encryption and decryption

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/encrypt>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/decrypt>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/AesGcmParams>

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

```
async function performEncryptionDecryptionWithAESGCM(sourceData,
cryptoKey) {
    let nonce = new Int32Array(12); //96 bits
    CRYPTO_OBJ.getRandomValues(nonce);
```



```

//See https://developer.mozilla.org/en-US/docs/Web/API/AesGcmParams
let additData = new Int32Array(16); //128 bits
CRYPTO_OBJ.getRandomValues(additData);
let aesGcmParams = {
  name: "AES-GCM",
  iv: nonce,
  additionalData: additData,
  tagLength: 128 //16 bytes
};
let dataEncoded = TEXT_ENCODER.encode(sourceData);
//See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/encrypt
let encryptedData = await CRYPTO_OBJ.subtle.encrypt(aesGcmParams,
cryptoKey, dataEncoded)
//See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/decrypt
let decryptedData = await CRYPTO_OBJ.subtle.decrypt(aesGcmParams,
cryptoKey, encryptedData)
let plainText = TEXT_DECODER.decode(decryptedData);
let result = {
  encryptedData: toHex(encryptedData),
  cycleSucceed: (sourceData === plainText)
}
return result;
}

```

HMAC

Source: <https://developer.mozilla.org/en-US/docs/Web/API/HmacKeyGenParams>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/generateKey>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/sign>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/verify>

⚠ For the generation of the secret, specify the member **length** of the [HmacKeyGenParams](https://developer.mozilla.org/en-US/docs/Web/API/HmacKeyGenParams) object, only if **you know what you are doing** from a cryptography point of view.

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

❗ This include the **secret** handling too.

```

async function performSecretGenerationForSignVerifyUsageWithHMAC() {
    //Generate a secret (cryptoKey) for HMAC operation with SHA-512
    //See https://developer.mozilla.org/en-US/docs/Web/API/HmacKeyGenParams
    let hmacKeyGenParams = {
        name: "HMAC",
        hash: "SHA-512"
    };
    let keyUsages = ["sign", "verify"];
    //See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/generateKey
    let cryptoKey = await CRYPTO_OBJ.subtle.generateKey(hmacKeyGenParams,
true, keyUsages);
    return cryptoKey;
}

async function performSignVerifyWithHMAC(sourceData, cryptoKey) {
    let algorithm = "HMAC";
    let dataEncoded = TEXT_ENCODER.encode(sourceData);
    //See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/sign
    let signature = await CRYPTO_OBJ.subtle.sign(algorithm, cryptoKey,
dataEncoded);
    //See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/verify
    let isValid = await CRYPTO_OBJ.subtle.verify(algorithm, cryptoKey,
signature, dataEncoded);
    let result = {
        signature: toHex(signature),
        cycleSucceed: isValid
    }
    return result;
}

```

Asymmetric key handling

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/generateKey>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/RsaHashedKeyGenParams>

Source: <https://www.keylength.com/en/3/>

⚠ For the generation of the key pair, specify for the member **publicExponent** of the [RsaHashedKeyGenParams](#) object another value than 65537 (`new Uint8Array([1, 0, 1])`), only if

you know what you are doing from a cryptography point of view.

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

```
async function
performAsymmetricKeyGenerationForEncryptionDecryptionUsageWithRSAOAEP() {
    //RSA was chosen because EC was not supported by the "algorithm"
    parameter at the time of the POC (June 2021):
    //See https://developer.mozilla.org/en-
    US/docs/Web/API/SubtleCrypto/encrypt#parameters
    //Generate a RSA-OAEP key pair with a size of 4096 bits
    //See https://developer.mozilla.org/en-
    US/docs/Web/API/RsaHashedKeyGenParams
    //See https://www.keylength.com/en/3/
    //See https://developer.mozilla.org/en-
    US/docs/Web/API/RsaHashedKeyGenParams#properties
    let rsaHashedKeyGenParams = {
        name: "RSA-OAEP",
        modulusLength: 4096,
        publicExponent: new Uint8Array([1, 0, 1]),
        hash: "SHA-512"
    };
    let keyUsages = ["encrypt", "decrypt"];
    //See https://developer.mozilla.org/en-
    US/docs/Web/API/SubtleCrypto/generateKey
    let cryptoKeyPair = await
    CRYPTO_OBJ.subtle.generateKey(rsaHashedKeyGenParams, true, keyUsages);
    return cryptoKeyPair;
}
```

Asymmetric encryption and decryption

Source: <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/encrypt>

Source: <https://developer.mozilla.org/en-US/docs/Web/API/RsaOaepParams>

Can be used in the context of the following protocols:

- HTTP: ✗
- HTTPS: ✓

Code snippet:

```

async function performEncryptionDecryptionWithRSAOAEP(sourceData,
cryptoKeyPairPublicKey, cryptoKeyPairPrivateKey) {
    let labelData = new Int32Array(32); //256 bits
    CRYPTO_OBJ.getRandomValues(labelData);
    //See https://developer.mozilla.org/en-US/docs/Web/API/RsaOaepParams
    let rsaOaepParams = {
        name: "RSA-OAEP",
        label: labelData
    };
    let dataEncoded = TEXT_ENCODER.encode(sourceData);
    //See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/encrypt
    let encryptedData = await CRYPTO_OBJ.subtle.encrypt(rsaOaepParams,
cryptoKeyPairPublicKey, dataEncoded)
    //See https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/decrypt
    let decryptedData = await CRYPTO_OBJ.subtle.decrypt(rsaOaepParams,
cryptoKeyPairPrivateKey, encryptedData)
    let plainText = TEXT_DECODER.decode(decryptedData);
    let result = {
        encryptedData: toHex(encryptedData),
        cycleSucceed: (sourceData === plainText)
    }
    return result;
}

```

💡 Observations:

- For the test cases above "100", the browser raise an operation specific error. This error is consistent because the amount of data is big for a asymmetric encryption operation. This behavior prevent the browser to hang or crash due to the launching of a huge processing.
- Asymmetric encryption is targeted for a small data like the protection of a symmetric key during the exchange for later symmetric encryption operation.
- If the following code is used, on Firefox (last version on June 2021) it continue to encrypt the data provided whatever the size and made the browser unstable:

```

function
performIdentificationOfContentLengthLimitForEncryptionWithRSAOAEP(cryptoKeyPairPublicKey) {
    let labelData = new Int32Array(32);
    CRYPTO_OBJ.getRandomValues(labelData);
    let rsaOaepParams = {
        name: "RSA-OAEP",

```

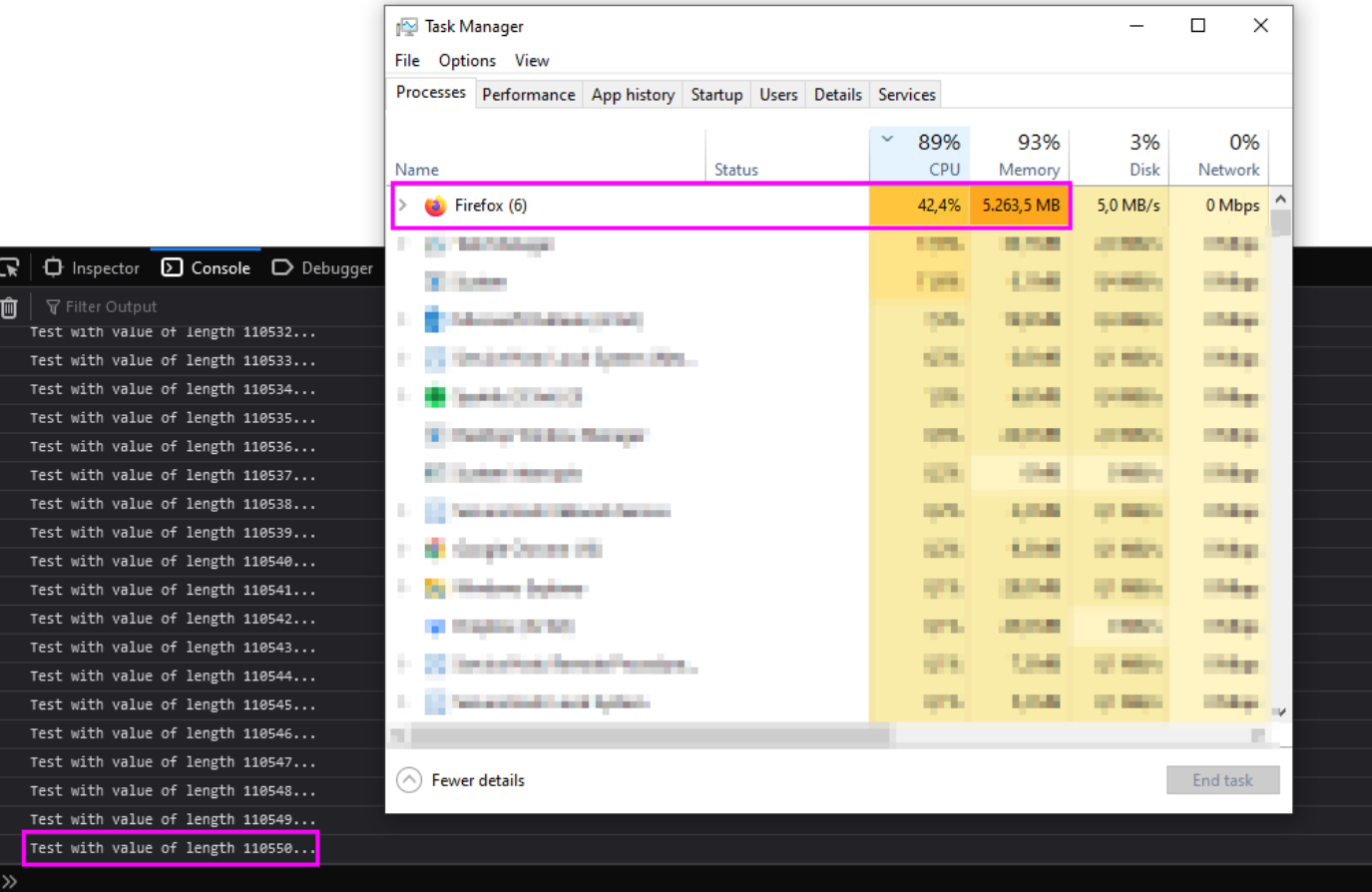
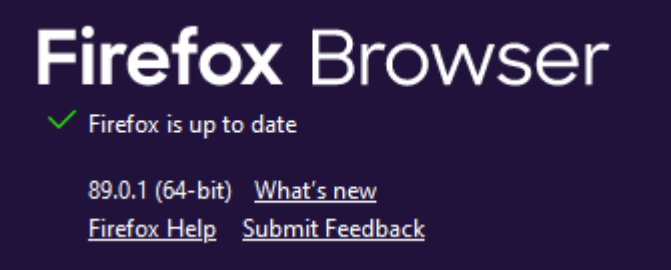
```

    label: labelData
  };

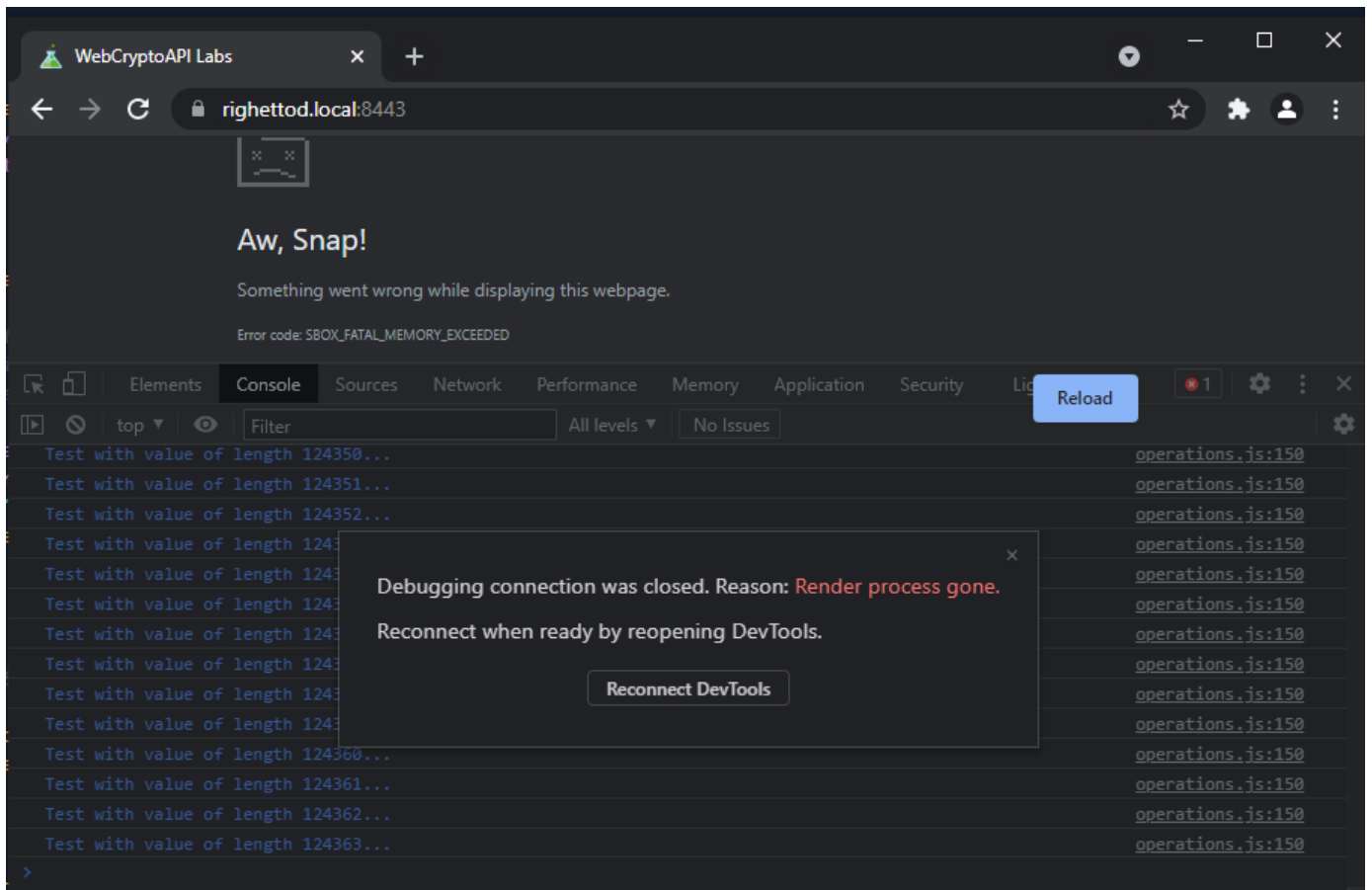
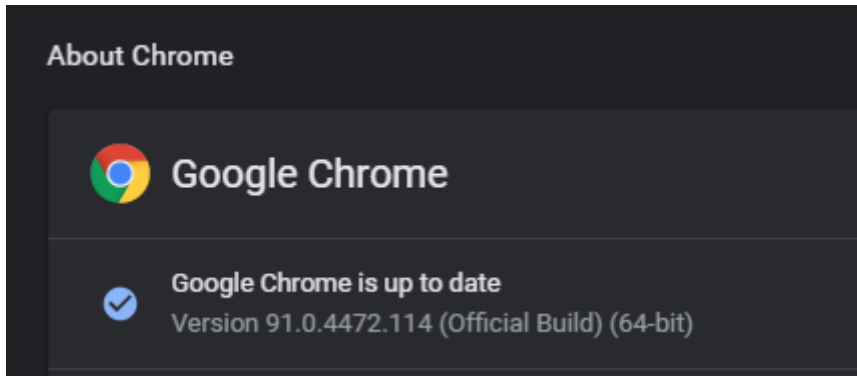
  let dataEncoded = null;
  for (let i = 100; i < 1000000; i++) {
    console.debug("Test with value of length " + i + "...");
    dataEncoded = TEXT_ENCODER.encode("T".repeat(i));
    CRYPTO_OBJ.subtle.encrypt(rsaOaepParams, cryptoKeyPairPublicKey,
dataEncoded).catch(err => {
      console.warn(err);
      return i;
    });
  }
}

```

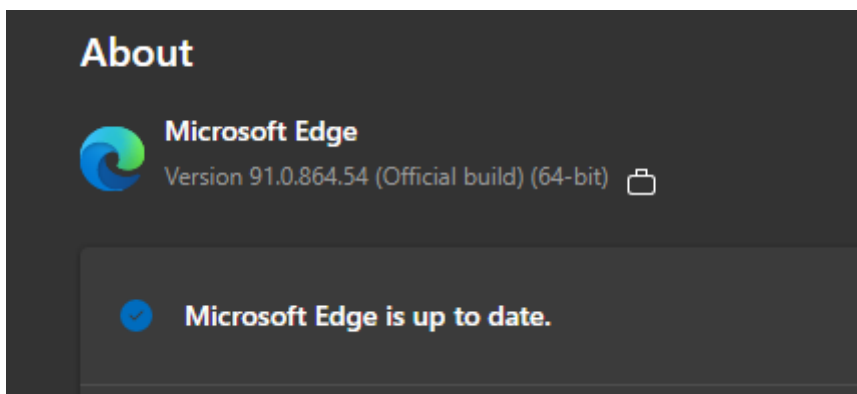
Run on Firefox my laptop, catch clause was not invoked and browser became unstable (kill of the tab required):

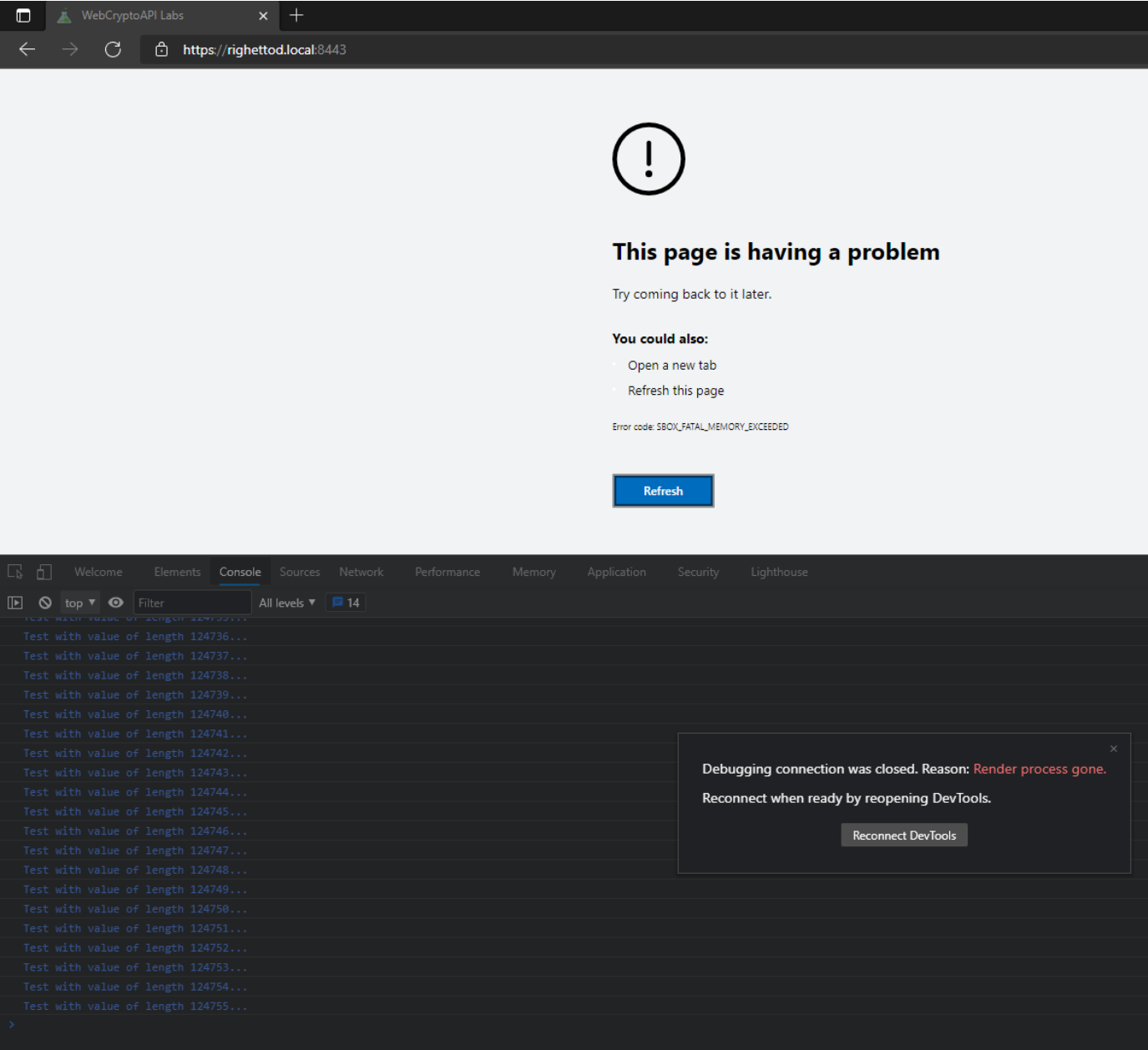


Same test on Chrome (last version on June 2021), browser stay stable and raise the following error without causing any instability:



Same behavior than Chrome on Edge (last version on June 2021):





Signature

⌘ TODO

Key import/export

⌘ TODO

Key derivation

⌘ TODO