**Практическое задание № 9**

**Тема «Изучение стандартных средств для реализации симметричного и ассиметричного шифрование с использованием SubtleCrypto в js»**

Цель: Изучить интерфейс **SubtleCrypto**, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования

**Криптография в Js**

Web Crypto API - это интерфейс, позволяющий использовать криптографические примитивы для построения систем с использованием криптографии. Данный интерфейс включают в себя возможность генерировать, использовать и применять пары криптографических ключей; шифровать и дешифровать сообщения; надежно генерировать случайные числа

Некоторые браузеры реализовали интерфейс под названием Crypto, без точной структуры. Чтобы избежать путаницы, методы и свойства этого интерфейса были удалены из браузеров, реализующих Web Crypto API, и все методы Web Crypto API доступны в новом интерфейсе: SubtleCrypto.

Интерфейс SubtleCrypto Web Crypto API предоставляет ряд низкоуровневых криптографических функций. Доступ к функциям SubtleCrypto осуществляется через объёкт Crypto.subtle .

Этот объект содержит набор методов для выполнения общих криптографических функций, таких как шифрование, хеширование, подписывание и генерация ключей. Поскольку все криптографические операции выполняются с необработанными двоичными данными, каждый метод SubtleCrypto имеет дело с типами ArrayBuffer и ArrayBufferView. Из-за того, что строки так часто становятся предметом криптографических операций, классы TextEncoder и TextDecoder будут часто использоваться вместе с SubtleCrypto для преобразования в строки и обратно.

Одной из проблем криптографии является генерация случайных чисел. Если будет использоватся Math.random() то будет сгенерировано псевдослучайное число которое использует генератор PRNG (pseudorandom number generator). Поскольку сгенерированное число внутреннее состояние PRNG то использование данного алгоритма для криптографии неприемлемо. Для решения данной задачи решить эту проблему, криптографически безопасный генератор псевдослучайных чисел (cryptographically secure pseudorandom number generator, CSPRNG) дополнительно включает в себя источник энтропии качестве входных данных, такие системных свойств, которые проявляют непредсказуемое поведение. Это алгоритм медленнее PRNG, но значения, генерируемые CSPRNG, являются остаточно непредсказуемыми для криптографических целей. Код для генерации несколких случайных чисел можно увидеть в листинге 1.

const array = new Uint8Array(1);

for (let i=0; i<5; ++i) {

console.log(crypto.getRandomValues(array));

}

Листинг 1 – Код генерации случайных чисел

**Хеширование**

Хеширование в SubtleCrypto представлено следующими алгоритмами.

* Sha1
* Sha256
* Sha385
* Sha512

Метод SubtleCrypto.digest() используется для создания хеша сообщения. Ниже представлен пример для хеширования сообщения представлен в листинге 2.

const text = 'Hash using sha256';

async function digestMessage(message) {

const encoder = new TextEncoder();

const data = encoder.encode(message);

const hash = await crypto.subtle.digest(**'SHA-256'**, data);

return hash;

}

digestMessage(text)

.then((digestBuffer) => console.log(digestBuffer.byteLength));

Листинг 2 – Пример хеширования данных

Как видно из примера выше то для указания алгоритма хеширования используется первый параметр. Также стоит упомянуть что результат хеширования обычно используется в 16-ой форме. Для преобразования стоит добавить код представленный в листинге 3.

const hashArray = Array.from(new Uint8Array(hash));

const hashHex = hashArray.map((b) => b.toString(16).padStart(2, '0')).join('');

return hashHex;

Листинг 3 – Пример преобразование хеша в 16-ричную форму.

**Генерация ключей**

Генерация случайного CryptoKey выполняется с помощью метода SubtleCrypto.generateKey(algorithm, extractable, keyUsages). В этот метод передается объект params, *указывающий целевой алгоритм, логическое значение,указывающее, должен ли ключ извлекаться из объекта CryptoKey, и массив строк — keyUsages, указывающий, с какими методами*

Поскольку разные алгоритмы используют разный набор данных для ключей то в первый параметр содержит сооствутсвующее название алгоритма.

* RSA (RSASSA-PKCS1-v1\_5, RSA-PSS, or RSA-OAEP )использует объект RsaHashedKeyGenParams.
* ECDSA и ECD Hи спользует объект EcKeyGenParams.
* HMAC использует объект HmacKeyGenParams.
* AES (AES-CTR, AES-CBC, AES-GCM, AES-KW) использует объект AesKeyGenParams

Значение extractable является логическим значением и указывает на возможность экспорта ключа.

Третий параметр keyUsages описывает, с какими алгоритмами можно использовать ключ.

* encrypt: Ключ используется для шифрования сообщений.
* decrypt: Ключ используется для расшифровки сообщений.
* sign: Ключ используется для подписи сообщений.
* verify: Ключ используется для проверки подписанного сообщения.
* deriveKey: Ключ используется для получения ключа.
* deriveBits: Ключ используется для получения битов.
* wrapKey: Ключ используется для упаковки ключа
* unwrapKey: Ключ используется для распоковки ключа.

Пример генерация ключа представлен в листинге 4.

(async function() {

const params = {

name: 'AES-CTR',

length: 128

};

const keyUsages = ['encrypt', 'decrypt'];

const key = await crypto.subtle.generateKey(params, false, keyUsages);

console.log(key);

})();

Листинг 4 – Пример генерации ключей.

**Шифрование и дешифрование**

Объект SubtleCrypto позволяет использовать как открытый ключ, так и симметричные алгоритмы для шифрования и дешифрования сообщений. Это может быть выполнено с использованием методов SubtleCrypto.encrypt() и SubtleCrypto.decrypt() соответственно. Ниже представлена часть кода для шифрования и дешифрования данных где algoIdentifier это название алгоритма и представлена в листинге 5.

const originalPlaintext = (new TextEncoder()).encode('Crypto');

const encryptDecryptParams = {

name: algoIdentifier,

iv: crypto.getRandomValues(new Uint8Array(16))

};

const ciphertext = await crypto.subtle.encrypt(encryptDecryptParams, key,

originalPlaintext);

console.log(ciphertext);

// ArrayBuffer(32) {}

const decryptedPlaintext = await crypto.subtle.decrypt(encryptDecryptParams,

key, ciphertext);

console.log((new TextDecoder()).decode(decryptedPlaintext));

Листинг 5 – Часть кода для шифрования и дешифрования.

**Создание цифровой подписи и проверка сообщений**

Объект SubtleCrypto позволяет использовать алгоритмы с открытым ключом для генерации подписей с использованием закрытого ключа или для проверки подписей с использованием открытого ключа. Они выполняются с использованием методов SubtleCrypto.sign() и SubtleCrypto.verify() соответственно. Для подписания сообщения требуется объект params, чтобы указать алгоритм и любые необходимые значения, частный CryptoKey и ArrayBuffer или ArrayBufferView для подписи. В примере, представленном в листинге 6 можно увидеть процесс создания цифровой подписи и проверки сообщения с цифровой подписью.

async function() {

const keyParams = {

name: 'ECDSA',

namedCurve: 'P-256'

};

const keyUsages = ['sign', 'verify'];

const {publicKey, privateKey} = await crypto.subtle.generateKey(keyParams,

true, keyUsages);

const message = (new TextEncoder()).encode('Mes to sign');

const signParams = {

name: 'ECDSA',

hash: 'SHA-256'

};

const signature = await crypto.subtle.sign(signParams, privateKey, message);

const verified = await crypto.subtle.verify(signParams, publicKey, signature,

message);

console.log(verified); // true

})();

Листинг 6 – Пример создания и проверки сообщений с цифровой подписью.

**Упаковка и распаковка ключа**

Объект SubtleCrypto позволяет упаковывать и распаковывать ключи, чтобы обеспечить передачу по ненадежному каналу. Это выполняется с использованием методов SubtleCrypto.wrapKey() и SubtleCrypto.unwrapKey() соответственно. Для переноса ключа требуется строка форматирования, экземпляр CryptoKey для переноса, CryptoKey для выполнения переноса и объект params для указания алгоритма и любых необходимых значений. В примере представленном в листинге 7 симметричный ключ AES-GCM, упаковывается с помощью AES-KW и, распаковывается обратно.

(async function() {

const keyFormat = 'raw';

const extractable = true;

const wrappingKeyAlgoIdentifier = 'AES-KW';

const wrappingKeyUsages = ['wrapKey', 'unwrapKey'];

const wrappingKeyParams = {

name: wrappingKeyAlgoIdentifier,

length: 256};

const keyAlgoIdentifier = 'AES-GCM';

const keyUsages = ['encrypt'];

const keyParams = {

name: keyAlgoIdentifier,

length: 256};

const wrappingKey = await crypto.subtle.generateKey(wrappingKeyParams,

extractable, wrappingKeyUsages);

console.log(wrappingKey);

const key = await crypto.subtle.generateKey(keyParams, extractable, keyUsages);

console.log(key);

const wrappedKey = await crypto.subtle.wrapKey(keyFormat, key, wrappingKey,

wrappingKeyAlgoIdentifier);

console.log(wrappedKey);

const unwrappedKey = await crypto.subtle.unwrapKey(keyFormat, wrappedKey,

wrappingKey, wrappingKeyParams, keyParams, extractable, keyUsages);

console.log(unwrappedKey);

})()

Листинг 7 – Пример упаковки и распаковки ключа.

Список литературы

[1] https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto

**Задание к выполнению:**

1. Ознакомиться с созданием криптографического приложения
2. Выполнить генерацию и вывод в консоль случайный чисел.
3. Выполнить шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам.

|  |  |  |
| --- | --- | --- |
| № | Алгоритм шифрования(размер ключа) | Алгоритм хеширования |
| 1 | RSA-OAEP | SHA-1 |
| 2 | AES-CTR | SHA-256 |
| 3 | AES-CBC | SHA-384 |
| 4 | AES-GCM | SHA-512 |
| 5 | AES-CTR | SHA-1 |
| 6 | AES-CBC | SHA-256 |
| 7 | AES-GCM | SHA-384 |
| 8 | RSA-OAEP | SHA-512 |
| 9 | AES-CBC | SHA-1 |
| 10 | AES-GCM | SHA-256 |
| 11 | RSA-OAEP | SHA-384 |
| 12 | AES-CTR | SHA-512 |
| 13 | AES-GCM | SHA-1 |
| 14 | RSA-OAEP | SHA-256 |
| 15 | AES-CTR | SHA-384 |

Если количество человек в группе больше 15 то номер варианта определяется как x=n mod 15 где n номер в списке. В случае номер варианта в ходе решения уравнения ровен 0 то номер варианта равен 15.

1. Продемонстрировать упаковку и распаковку ключа, полученного в предыдущем задании используя алгоритм AES-KW.
2. Выполнить процедуру подписи сообщения и проверку подлинности с использованием RSA-PSS или ECDSA на выбор.