Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №9**

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

Руководитель: Ржеутская Н. В.

Выполнил:

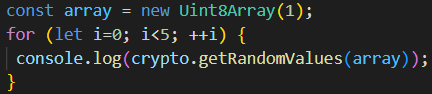
Студент 2 курса 8 группы ФИТ

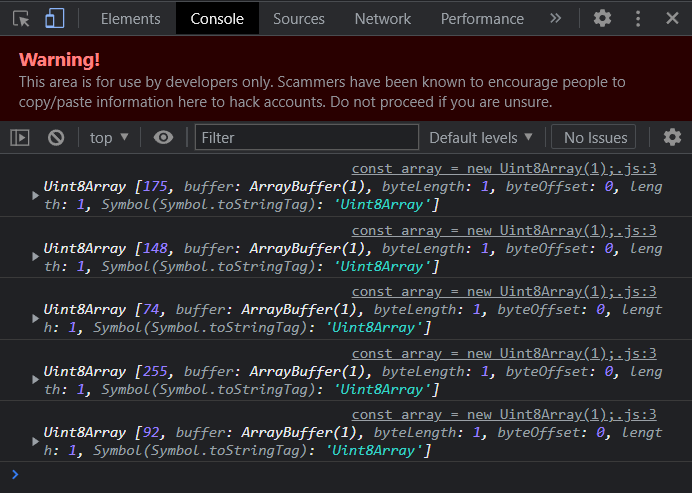
Солодкий Денис Викторович

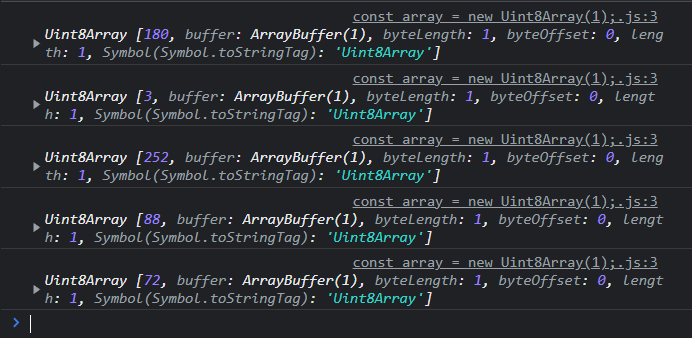
Минск 2022

**Задание №1**

Выполнить генерацию и вывод в консоль случайный чисел.



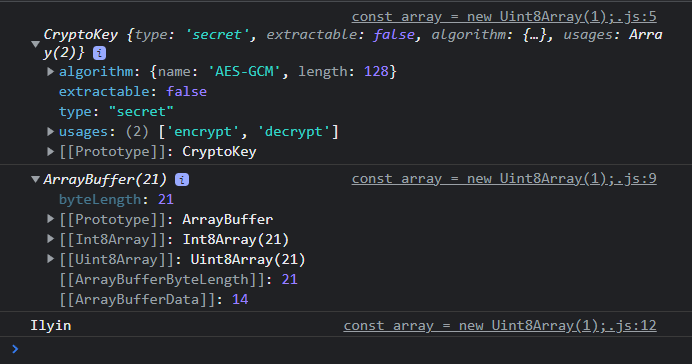


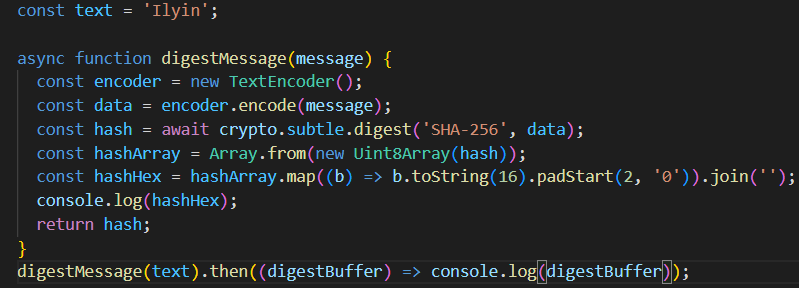


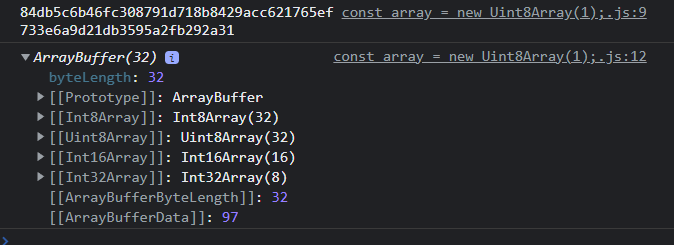
**Задание №2**

Выполнить шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам.



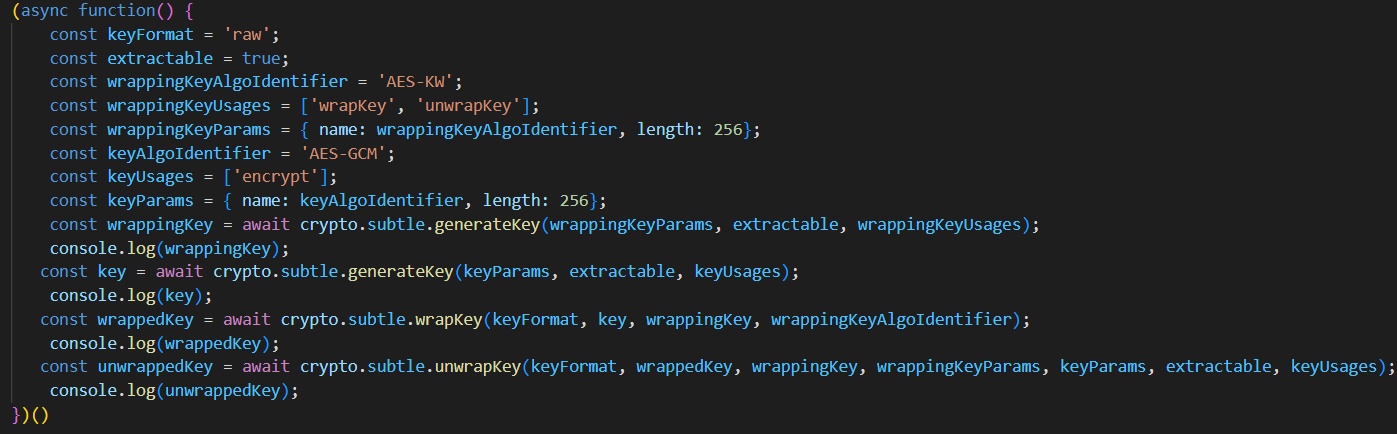






**Задание №3**

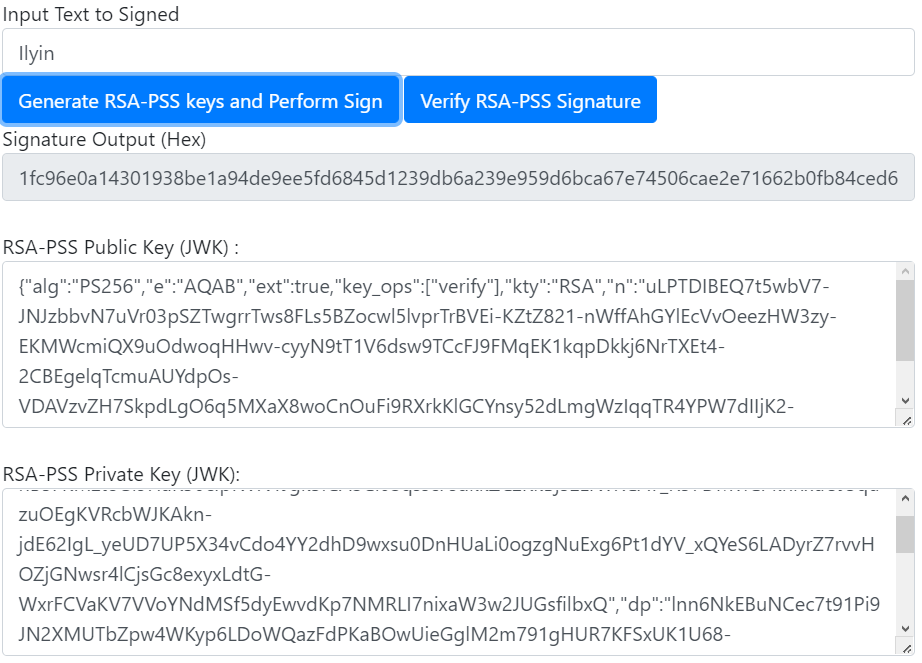
Продемонстрировать упаковку и распаковку ключа, полученного в предыдущем задании используя алгоритм AES-KW.

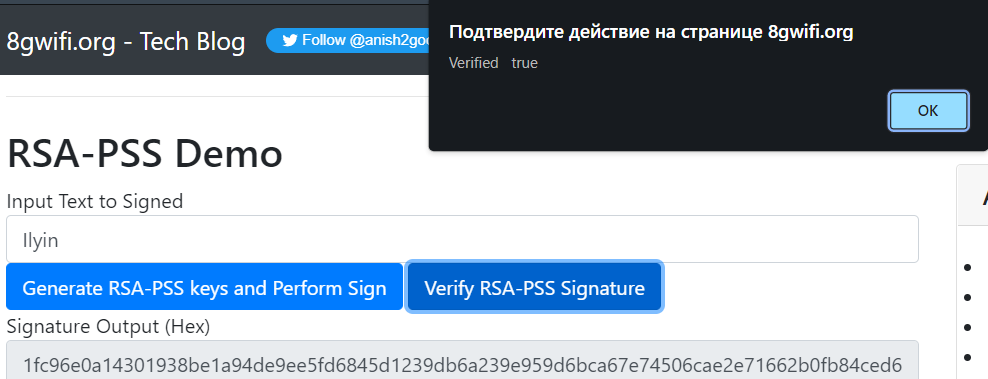


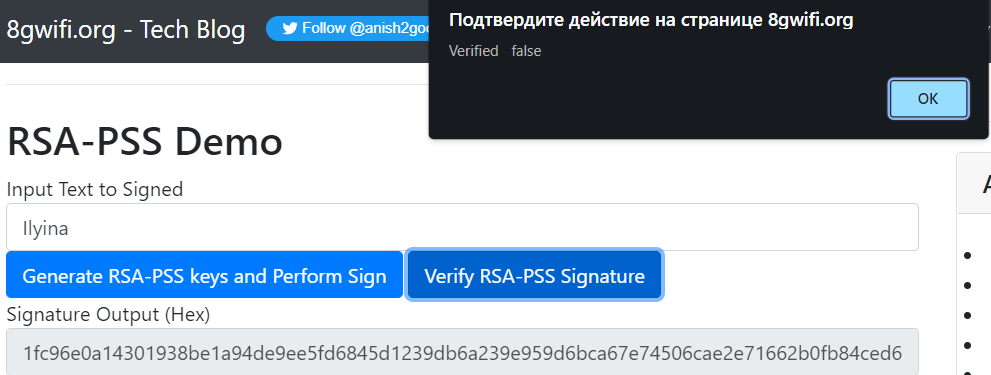


**Задание №4**

Выполнить процедуру подписи сообщения и проверку подлинности с использованием RSA-PSS или ECDSA на выбор.







**Вывод:** Web Crypto API – это интерфейс, позволяющий использовать криптографические примитивы для построения систем с использованием криптографии. Данный интерфейс включает в себя возможность генерировать, использовать и применять пары криптографических ключей; шифровать и дешифровать сообщения; надежно генерировать случайные числа. Существует множество алгоритмов шифрования, однако каждый из них отличается своей надёжностью. Если безопасность данных жизненно необходима, можно воспользоваться алгоритмом SHA-256. Упаковка и распаковка ключей используется для обеспечения безопасной и надёжной передачи данных по незащищённому каналу.