МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование асимметричных шифров»**

Студент:

Борисов Антон Андреевич

Вариант 1

Преподаватель:

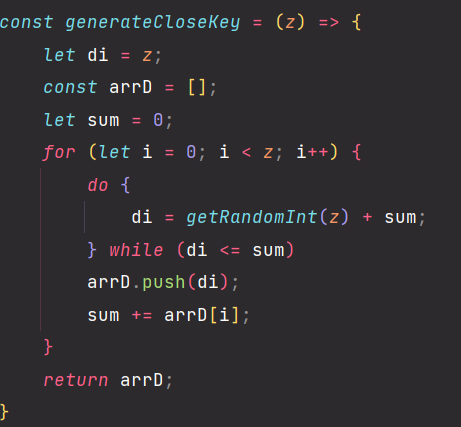
Блинова Евгения Александровна

Минск 2021

**ЗАДАНИЕ 1.** Алгоритм Меркла - Хеллмана

В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для расшифрования (тайный ключ).

В качестве закрытого ключа d (легкого для укладки ранца) используется сверхвозрастающая последовательность, состоящая из z элементов: d1, d2,..., dz: d = {di}, i = 1,..., z. Генерация сверхвозрастающей последовательности представлена ниже.



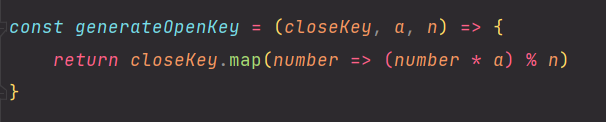
**Сверхвозрастающей** называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

Открытый ключ **e** представляет собой нормальную (не сверхвозрастающую) последовательность. Он формируется на основе закрытого ключа и не позволяет легко решить задачу об укладке ранца.

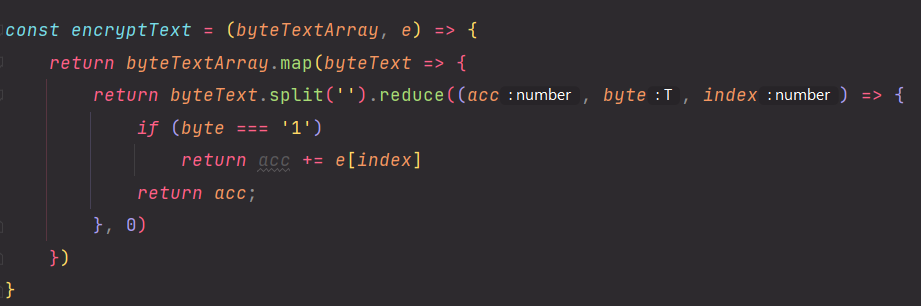
Для получения открытого ключа e (e = {ei}, i = 1,..., z) все значения закры- того ключа умножаются на некоторое число a по модулю n:

*ei = di a (mod n).*

Значение модуля n должно быть больше суммы всех чисел последова- тельности; кроме того, НОД (а, n) = 1.



Для зашифрования сообщения (М) оно сначала разбивается на блоки, по размерам равные числу (z) элементов последовательности в ранце. Затем, счи-тая, что 1 указывает на присутствие элемента последовательности в ранце, а 0 – на его отсутствие, вычисляются полные веса рюкзаков (Si, i = 1, . . ., z): по одному ранцу для каждого блока сообщения с использованием открытого ключа получателя, e. Реализация зашифрования.

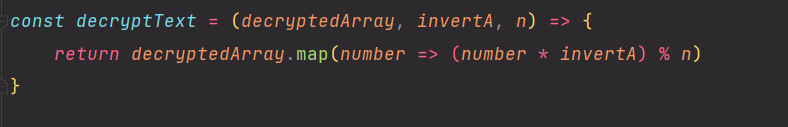


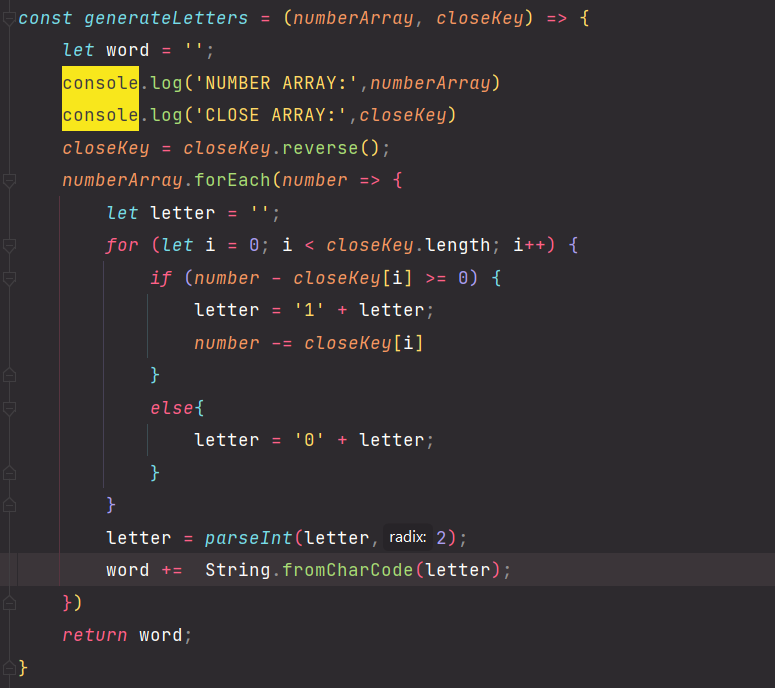
Для расшифрования сообщения получатель (использует свой тайный ключ, d: сверхвозрастающую последовательность) должен сначала определить обратное к a число, такое что: *а а-1(mod n) = 1.*

После определения обратного числа каждое значение шифрограммы (ci) преобразуется в соответствии со следующим соотношением:

*Si = ci а-1 mod n.*

Полученное на основании последней формулы для каждого блока число далее рассматривается как заданный вес ранца, который следует упаковать по изложенному выше алгоритму, используя сверхвозрастающую последователь- ность (тайный ключ получателя).





Результат выполнения программы представлен ниже.

