Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЁТ

по практическому заданию №4

Тема работы: Электронная цифровая подпись

Выполнил

Проверил Болтак С.В.

Минск 2023

## Ограничения

Числа p, q, h, x, k необходимо подобрать так, чтобы они удовлетворяли определенным условиям, иначе программа не будет корректно подписывать и проверять файлы. Условия такие:

* Q – простое;
* P – простое, причём, если вычесть единицу, то делится на Q;
* H – число из интервала от 1 до P – 1;
* X – число из интервала от 0 до Q;
* G = H ^ ((P-1)/Q) mod P > 1.

Поскольку подобрать числа, удовлетворяющие всем требованиям сразу, не так просто, программа при запуске заполняет поля корректными числами по умолчанию.

## Функционал

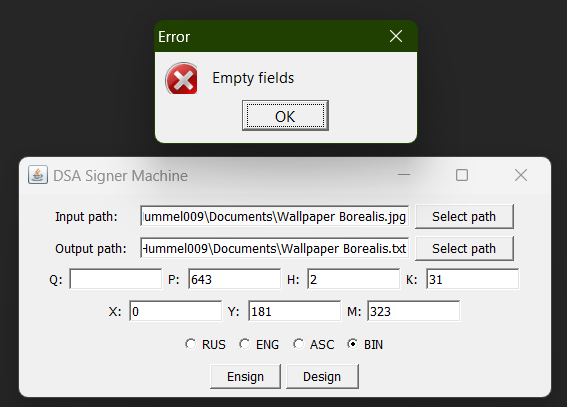
Исходя из методического пособия, а также условия задачи, было реализовано четыре режима подписи файлов, в которых применяются разные алгоритмы хеширования и проставления самой подписи:

* RUS: показанный в методическом пособии вариант. Работает с текстовыми файлами с кириллическим текстом. Буквы в тексте заменяются на их позицию в алфавите, после чего начинается хеширование. Нулевой символ алфавита – пробел;
* ENG: отличается от первого варианта лишь тем, что буквы в документе должны быть латинскими;
* ASC: вариант для текстовых файлов, в которых могут быть различные символы. Здесь буквы заменяются не на позицию в алфавите, а на кодовое значение символа;
* BIN: вариант для бинарных файлов. Обрабатывает что угодно, в том числе текстовые файлы. Воспринимает файл как последовательность чисел-байт.

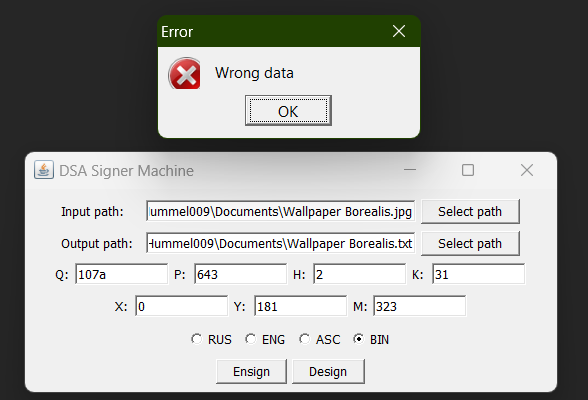
В программе также можно ввести с клавиатуры число M – число, на которое будет производиться деление в алгоритме хеширования.

## Тестирование ошибочных ситуаций

Программа не позволяет начать обработку, если файл для подписи и файл для сохранения не выбран.



Программа также не сработает, если ввести не числа или же ввести числа, не удовлетворяющие правилам, указанным в разделе «Описание».



Если же файлы выбраны и числа подходят, то программа успешно выполняет подпись/проверку подписи.

