**Задание:** Разработать приложение, реализующее хеширование сообщений.

**Электронная цифровая подпись** (ЭЦП) – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

ЭЦП представляет из себя бинарную последовательность, позволяющую однозначно идентифицировать отправителя.

Как правило, ЭЦП вычисляется на основе хеша подписываемого сообщения.

То есть подпись зависит от содержания того, что ей подписывается.

**ЭЦП на основе RSA**

ЭЦП на основе RSA вычисляется по следующей формуле:

Где *d* и *n* – элементы тайного ключа отправителя,

H – хеш-функция,

*M* – сообщение.

При получении подписанного сообщения пользователь вычисляет H(*M*) и сравнивает его со значением:

Где *S* – подпись,

*e* и *n* – элементы открытого ключа отправителя.

Если H(*M*) и H’(*M*) совпадают, значит авторство отправителя подтверждено.

**ЭЦП на основе Эль-Гамаля**

За основу берётся алгоритм асинхронного шифрования Эль-Гамаля. При вычислении используется случайное число *k*, взаимно простое с *p – 1* (*p* – элемент ключевой информации в алгоритме Эль-Гамаля). ЭЦП состоит из двух блоков (*a* и *b*), вычисляемых по формулам:

Где *g, p, x* – элементы тайного ключа отправителя,

H – хеш-функция,

*M* – сообщение,

*a* – первый блок ЭЦП,

*b* – второй блок ЭЦП.

При получении подписанного сообщения пользователь вычисляет 2 параметра:

Где g, p, y – элементы открытого ключа отправителя,

H – хеш-функция,

*M* – сообщение,

*a* – первый блок ЭЦП,

*b* – второй блок ЭЦП.

Если значения *V* и *W*, совпадают, то отправитель верифицирован.

Класс на Python, реализующий ЭЦП на основе Эль-Гамаля:

**ЭЦП Шнорра**

ЭЦП Шнорра является вариантом алгоритма Эль-Гамаля. Подпись также состоит из двух блоков (*h* и *b*), но они вычисляются по другим формулам:

Где *p, g, q, x* – элементы тайного ключа отправителя,

*k* – случайное число, взаимно простое с *p – 1*,

H – хеш-функция,

*M* – сообщение.

При получении подписанного сообщения пользователь вычисляет параметр *X*:

Где p, g, y – элементы публичного ключа отправителя.

Если значение параметра *X* совпадает со значением блока *h* ЭЦП, отправитель верифицирован.

Класс на Python, реализующий ЭЦП Шнорра: