Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование асимметричных шифров RSA и Эль-Гамаля

Студент: Точило О. В.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

# **Алгоритм RSA**

Для генерации двух ключей: тайного и открытого (а по сути – двух взаимосвязанных частей одного ключа, т. е. ключа, принадлежащего одному физическому лицу (или группе лиц), либо одному юридическому лицу), используются два больших случайных простых числа *p* и *q*. Для максимальной большей криптостойкости нужно выбирать *p* и *q* равной длины. Рассчитывается произведение: *n* = *pq*. Это есть один из трех компонент ключа, состоящего из чисел *n*, *e*, *d*.

Затем случайным образом выбирается второй компонент ключа (открытый ключ или ключ зашифрования, *e*, такой что *e* и (*p* – 1)(*q* – 1) являются взаимно простыми числами; вспомним, что (*p* – 1)(*q* – 1) = φ(*n*) – функция Эйлера).

Наконец, расширенный алгоритм Евклида используется для вычисления третьего компонента ключа: ключа расшифрования *d* такого, что выполняется условие:



Таким образом, сформирован ключ, состоящий из трех чисел, которые в свою очередь образуют две вышеупомянутые взаимосвязанные части: открытый (публичный) ключ (*e*, *n*) и тайный ключ (*d*, *n*; на самом деле, как видим, тайным здесь является лишь первое из пары чисел).

Для зашифрования/расшифрования используется ключ получателя: отправитель шифрует сообщение открытым ключом, а получатель расшифровывает шифртекст своим тайным ключом.

# **Зашифрование алгоритмом RSA**

Если шифруется сообщение *М*, состоящее из r блоков: *m1*, *m2*, …, *mi*, …, *mr*, то шифртекст *С* будет состоять из такого же числа блоков, представляемых числами:



Для зашифрования используется следующий метод, представленный на рисунке 1.1.

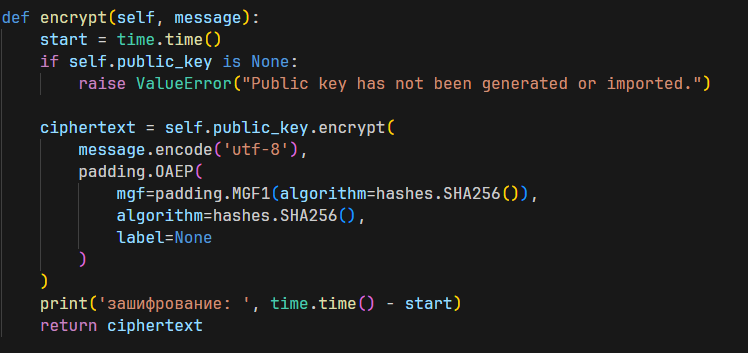


Рисунок 1.1 – Функция зашифрования алгоритмом RSA

# **Расшифрование алгоритмом RSA**

Для расшифрования каждого зашифрованного блока производится вычисление вида:



Код функции для расшифрования представлен на рисунке 1.2.

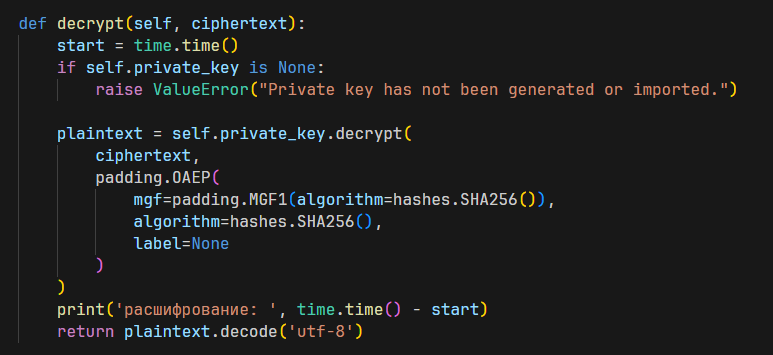


Рисунок 1.2 – Функция расшифрования алгоритмом RSA

# **Алгоритм Эль-Гамаля**

Генерация ключевой информации. Выбирается простое число *р*. Выбирается число (*g*, *g* < *p*), являющееся первообразным корнем числа *р* – очень важный элемент с точки зрения безопасности алгоритма. Далее выбирается число *х* (*х* < *p*) и вычисляется последний компонент ключевой информации:



Владельцу сформированной ключевой информации, состоящей из 4 чисел, может посылаться некоторый шифртекст, созданный с использованием открытого ключа получателя: *p*, *g*, *y*. Расшифрование шифртекста получатель производит своим тайным ключом: *p*, *g*, *х*. Как видим, на самом деле тайным является лишь одно число (как и в RSA): *х*.

# **Зашифрование алгоритмом Эль-Гамаля**

Для зашифрования алгоритмом Эль-Гамаля реализован код функции, представленной на рисунке 2.1.

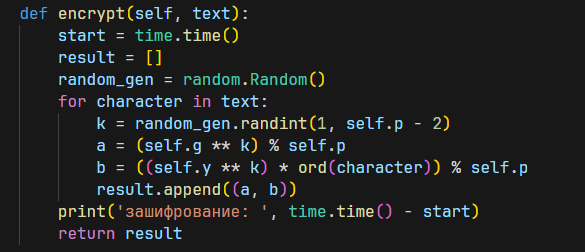


Рисунок 2.1 – Функция зашифрования алгоритмом Эль-Гамаля

# **Расшифрование алгоритмом Эль-Гамаля**

Для расшифрования реализована следующая функция, представленная на рисунке 2.2.

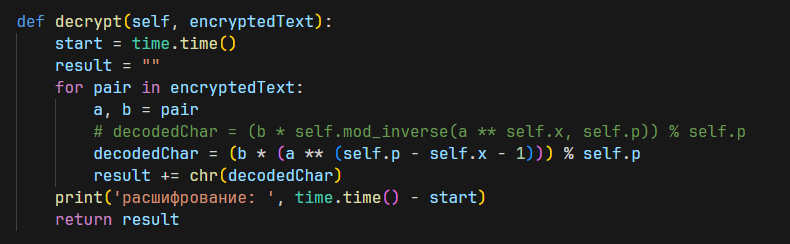


Рисунок 2.2 – Функция расшифрования алгоритмом Эль-Гамаля

# **Вывод**

В данный лабораторной работе были изучены и приобретены практические навыки разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.