Отчет по лабораторной работе 8

Даниил Генералов, 1032212280

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Выполнение лабораторной работы

Сначала нам потребуется программа, которая позволяет сделать XOR-шифрование между двумя байтовыми строками, а также шаблон, который позволяет нам определить общие компоненты между двумя сообщениями. Это – те шаги, которые предпринимает пользователь криптосистемы: та информация, которая ему доступна, видна на fig. 2.1.

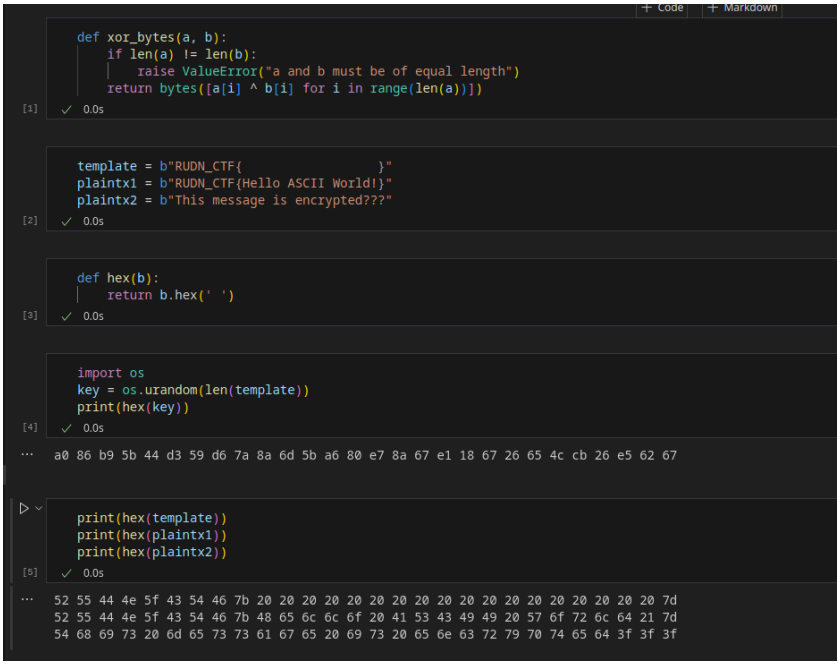

Рис. 2.1: plaintext, template и ключ

После этого злоумышленник получает доступ к двум шифртекстам и исходному тексту шаблона. Сделав XOR между двумя шифртекстами, мы получаем нули там, где эти два шифртекста совпадают – это либо те байты, которые являются частью шаблона, либо те, которые повторяются между двумя шифртекстами.

Затем, сделав XOR между этим и шаблоном, можно найти те слова, которые могут быть частью исходного текста (рис. fig. 2.2).

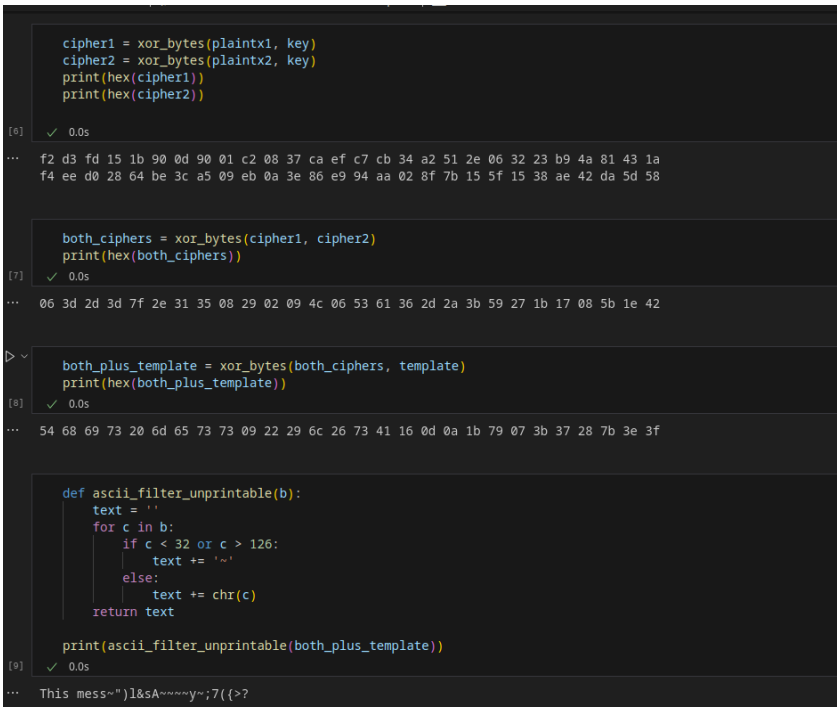

Рис. 2.2: xor шифртекстов

Можно затем попробовать этот процесс несколько раз, чтобы отгадывать больше частей исходного сообщения: подставлять угаданные куски, затем делать XOR, и смотреть какие части остаются.

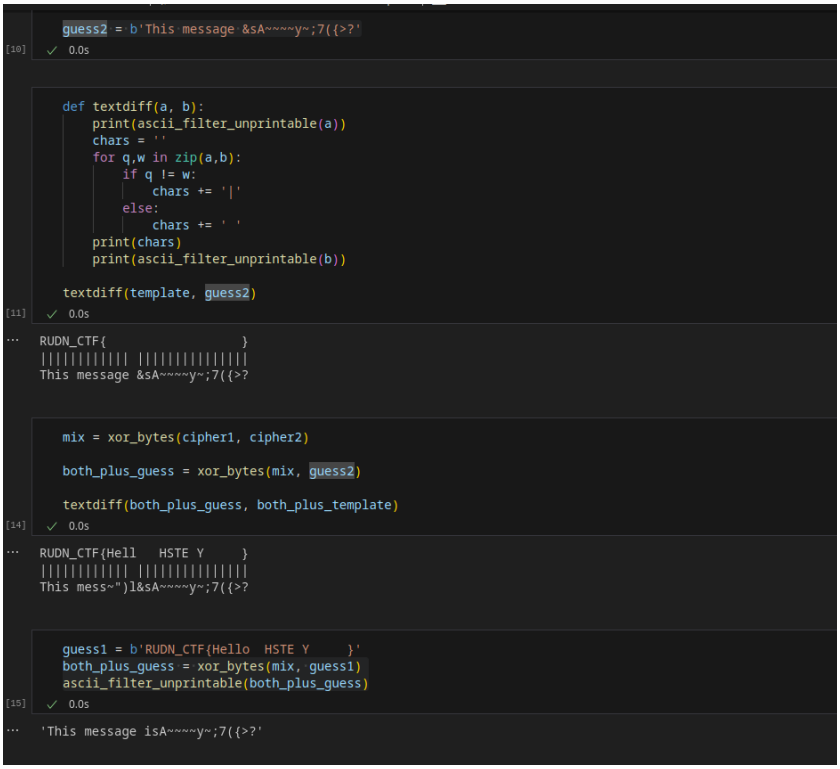

Рис. 2.3: изменение угаданного текста

Постепенно, смешивая шифртекст со своим предсказанием, мы можем получить исходные тексты обоих сообщений на рис. fig. 2.4. Зная исходные тексты и шифртексты, мы можем определить ключ, и затем разшифровывать любые другие сообщения, которые зашифрованы этим ключом (а также генерировать собственные).

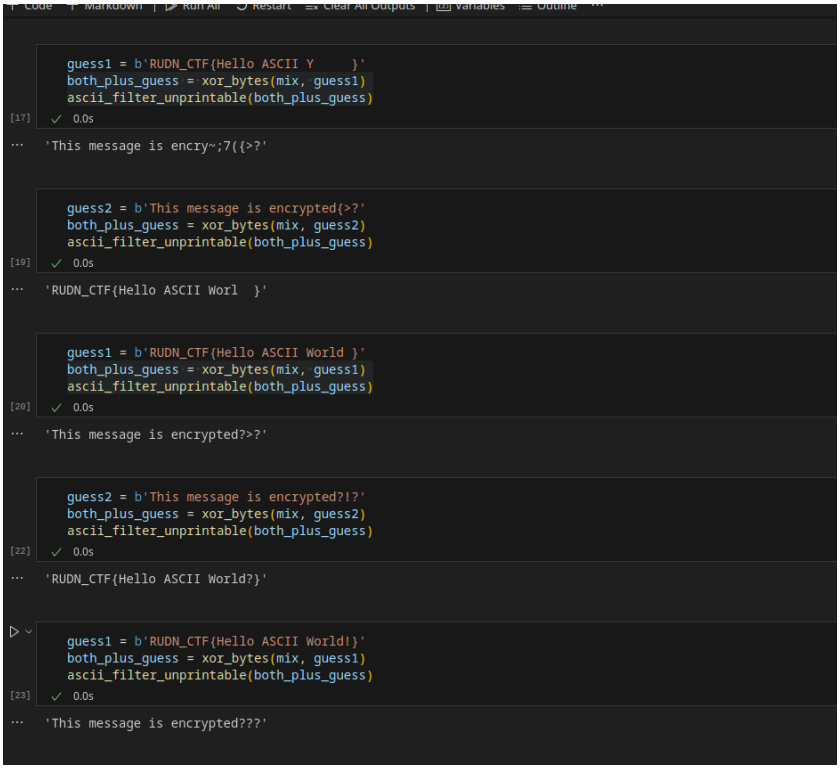

Рис. 2.4: определение исходного текста

3 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Если известен один шифртекст и его связанный исходный текст, то можно сделать XOR между ними, чтобы определить ключ. После этого можно использовать этот ключ, чтобы разшифровать другой шифртекст.

2. Что будет при повторном использовании ключа при шифровании текста?

Злоумышленник, наблюдающий оба шифртекста, может определить части исходного текста этих сообщений.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

После обычного шифрования используемый ключ не выбрасывается, а используется для шифрования второго текста.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Как мы показали в этой лабораторной работе, самым большим недостатком этой схемы является то, что злоумышленник, наблюдающий оба шифртекста, может определить исходный текст сообщений.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Для этого шифрования можно использовать один и тот же ключ. Поскольку в режиме однократного гаммирования длина ключа равна длине сообщения, то использование одного и того же ключа позволяет минимизировать количество общих данных.

4 Выводы

В этой лабораторной работе мы рассмотрели алгоритм однократного гаммирования и показали его слабость в случае, когда один и тот же ключ используется больше одного раза.