1 Description

Title: RSA на бумаге

Category: Crypto

Value: 300

Дан файл, зашифрованный с помощью RSA и публичный ключ, с помощью которого производилось шифрование. В комплекте идет фотография, распечатанного на бумаге приватного RSA ключа, который частично поврежден.

2 Legend

Инопланетный разум использует исключительно RSA для шифрования своей переписки. Нашему агенту удалось сфотографировать ключ через иллюминатор космического корабля.

3 Flag

Flag regex:	simple text
Flag:	whyplutoisnotaplanetanymore

4 Solution

Применяем стандартную атаку ферма на RSA. Придется постараться, чтобы распознать все символы ключа автоматически т.к. изображение достаточно большое. По ключу видно, что в нем много нулей, и его p и q вероятно очень близко друг к другу расположены. Поврежденный на картинке символ придется перебрать. Для перевода из PEM формата ключа можно воспользоваться библиотекой pycrypto или openssl.

5 Hints

1. Присмотритесь к ключу, почему он такой неслучайный.
2. PEM формат, если что.
3. Атака как по википедии.

6 Discussion

Никаких особых дополнений.

7 Setup

Выдать командам архив с файлами encrypted.enc, photo.jpg.