LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Cryptography and Security
`http://lasec.epfl.ch/`

Homework 3 - RSA Cryptography

Cryptography and Security 2018

- You are free to use any programming language you want, although SAGE is recommended.

- Put all your answers **and only your answers** in the provided SCIPER-answers.txt file. This means you need to provide us with Q_1, Q_2, Q_3, Q_4, Q_{5a}, Q_{5b} and Q_{5c}. You can download your **personal** files on `http://lasec.epfl.ch/courses/cs18/hw3/index.php`

- The answers Q_1 and Q_4 should be integers, the answer Q_2 should be a list of integers, the answer Q_3 should be an English phrase in ASCII, and the answers Q_{5a}, Q_{5b} and Q_{5c} should be tuples of integer. **Please provide nothing else. This means, we don't want any comment and any strange character or any new line** in the .txt file.

- We also ask you to submit your **source code**. This file can of course be of any readable format, although we prefer a textile with a Sage (python) script. We encourage you to comment your code.

- The plaintexts of most of the exercises contain some random words. Don't be offended by them and Google them at your own risk. Note that they might be really strange.

- If you worked with some other people, please list all the names in your answer file. We remind you that you have to submit your own source code and solution.

- We might announce some typos of this homework on Moodle in the "news" forum. Everybody is subscribed to it and does receive an email as well. If you decided to ignore Moodle emails we recommend that you check the forum regularly.

- The homework is due on Moodle on **Monday the 12th of November** at 22h00.

Exercise 1 Let's use the same primes!

Let $[k]$ denote the set $\{1, 2, \ldots, k\} \subset \mathbb{Z}$. For the rest of the exercise, you can assume that k is chosen in such a way that it is feasible to traverse/enumerate each element of $[k]$. Moreover, with abuse of notation we consider *greatest common divisor* gcd as a function, mapping finite sets of integers into integers:

$$\gcd : \{S : S \subset \mathbb{Z}\} \to \mathbb{Z}$$

For instance, if $S = \{2, 4, 9\}$, we can write $\gcd(S) = 1$. Let $\{r_i\}_{i=1}^{\ell}$ be a shorthand for $\{r_1, r_2, \ldots, r_\ell\}$.

Let p and q be two sufficiently large strong primes[1] and $N = p \cdot q$. Let x be an uniformly sampled element from $\mathbb{Z}_N$.

Consider a set of ℓ small odd integers $R = \{r_i\}_{i=1}^{\ell} \subseteq [k]$. Then we define x's R-th power as $S_x^R = \{x^{r_i} \bmod N\}_{i=1}^{\ell}$. You are given access to an oracle with fixed x value at `lasecpc28.epfl.ch:5557`, which samples $(r_i, x^{r_i}) \in [k] \times Z_N^*$ pairs (with unknown non-uniform distribution).

In your parameter file you will find (N_1, k_1) (k_1 is given for convenience). Your task is to recover x and provide it as Q_1 in your answer file.

Hint: Consider the relation among elements of R. With enough number of queries, the oracle will allow you to obtain set R such that $\gcd(R) = 1$?

You have access to the oracle at web interface `http://lasec.epfl.ch/courses/cs18/hw3/sampletuple.php`. Alternatively, you can connect to the server lasecpc28.epfl.ch on port 5557 using Sage or ncat to issue queries directly (see instructions above). Your query should consist of a single argument: your SCIPER number. An example from shell would be:

```
echo 123456 | ncat lasecpc28.epfl.ch 5557
```

which returns two integer values with a space in-between:

```
82447365 46494009989130606873625181766035642062178863925410660917534584694368
43822833895327077400584138899887303435439475468145817356893685082647317748433
095680
```

If you want to simplify things even further, consider using **the sage script provided on moodle page** (`sampletuple.sage`). Do not forget to update it with your own SCIPER number.

Exercise 2 Elements of order 2

In your parameter file, you can find the modulus n_2 and its factorization p_2, q_2, r_2 and s_2. Find all elements in $\mathbb{Z}_{n_2}^*$ which has the order 2, and write them in Q_2 in your answer file in increasing order.
Hint: 1 has the order 1.

Exercise 3 RSA with subgroup

After his failure with the ElGamal cryptosystem, the crypto-apprentice became very careful with the plaintext space. This time he decided to use the RSA encryption. The crypto-apprentice realized that one can apply similar attack to the RSA encryption, namely one can guess the encrypted message if the order of the message is small in $\mathbb{Z}_{n_3}$ where n_3 is the RSA modulus. In order to overcome this problem, the crypto-apprentice decided to use a generator of a subgroup.

After the RSA key generation, the receiver picks a generator g_3 which generates a subgroup of large order in $\mathbb{Z}_{n_3}$. Then, g_3 is sent through a confidential channel to the sender. Given a message $m = m_0 || m_1 || \cdots || m_{k_3 - 1}$ which consists of the lower case alphabet and the space, the encryption of the message is $c = [c_0, c_1, \cdots, c_{k_3-1}]$ where $c_i = \mathsf{RSA.Enc}(pk_3, g_3^{\mathsf{Encode}(m_i)})$ for $i \in \{0, \cdots, k_3 - 1\}$, pk_3 is the RSA public key of the receiver and Encode is a function which maps '␣' to 1, 'a' to 2, ..., 'z' to 27.

[1] As before, p is a strong prime if $\frac{p-1}{2}$ is prime too.

In your parameter file, you will find the modulus n_3 and the ciphertext c_3. Recover the secret message Q_3 and write it in your answer file. (This means that we expect a **"meaningful" English phrase in ASCII characters**!)

Exercise 4 (S)he who gets the orders knows the factors

Suppose that N is an RSA number (N_4 in parameter file), i.e. multiplication of two different large primes p and q such that $p < q$.

Briefly, you are given an access to an oracle which allows you to submit an element $x \in \mathbb{Z}_{N^2}^*$, whose order in $\mathbb{Z}_{N^2}^*$ will be returned. Namely, you will receive the smallest positive integer k such that $x^k \equiv 1 \pmod{N^2}$.

Your goal is to recover the smaller factor p (Beware: you will lose points if you return the large one). Provide your answer as Q_4 in your parameter file.

You have access to the oracle at web interface `http://lasec.epfl.ch/courses/cs18/hw3/order.php`. Alternatively, you can connect to the server lasecpc28.epfl.ch on port 5556 using Sage or ncat to issue queries directly (see instructions above). Your query should consist of two arguments: your SCIPER number and positive integer x (the oracle finds $x \mod N^2$ before doing anything else so any integer query should be valid). An example from shell would be:

```
echo 123456 2 | ncat lasecpc28.epfl.ch 5556
```

which returns the concatenated value of which is 512 characters long as below:

```
21345678976543245678973l2543
```

Again, you can use `sampletuple.sage` script by updating the port number.

Exercise 5 Diffie-Hellman With A Weird Group:

Our curious crypto-apprentice has got very interested in an implementation of Diffie-Hellman (DH) key exchange protocol. More precisely, she got curious about Alice and Bob using the DH key-exchange protocol on a very "exotic group". When the apprentice read the details of their protocol, she found out that they define their own group G with the set $\mathbb{Z}_{p_5}^* \times \mathbb{Z}_{p_5}$ and the following group law

$$\forall (a,u),(b,v) \in G; \quad (a,u) * (b,v) = (ab, bu + av).$$

She first wondered if G really defines a group! While showing that, she intercepted some of the public keys of Alice and Bob during the exchange! The more she pondered on the group G, the more she ssaw the wekaness of DH on the group G. Finally, our smart apprentice was able to figure out how to generate the shared secret key between Alice and Bob by just observing their public keys. But... How is that possible? Did she solve the discrete-log problem?

In this homework, you are asked to investigate this exotic DH key-exchange protocol. In your parameter file, you will find p_5, a_5, u_5, X_5 and Y_5.

1. Find the neutral element of G and write it down in your answer file under Q_{5a}.

2. In your parameter file, you will find a random element $(a_5, u_5) \in G$. Write down its inverse under Q_{5b}.

3. The generator of G for this specific DH protocol is in the form of $g = (2, \mathit{sciper})$. You will find your generator in your parameter file. You are also given a pair of intercepted public keys of Alice and Bob as $X_5 = g^x$ and $Y_5 = g^y$. Find the shared secret of Alice and Bob generated with g, X and Y, meaning that find g^{xy}. Write it down under Q_{5c}.