Security

Assignment 14, Wednesday, January 6, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, January 14, 23:59 (midnight) sharp!

Goals: After completing these exercises successfully, you should be able to

- understand when to compute in which group (i.e. modulo what value);
- perform necessary computations for creating and verifying ElGamal signatures;
- understand the dangers involved in reusing randomness;
- perform Bitcoin transactions.

Marks: You can score a total of 100 points.

1. **(30 points)** To better understand the modular computations used in discrete log problems, we solve the following toy exercise. Let $p = 43$ and $g = 11$.

   (a) Compute all powers of g modulo p (i.e. $g^1, g^2, g^3 \ldots$) until you get 1. Note that $g^2 = g \cdot g$, $g^3 = g^2 \cdot g$ etc.

   (b) How many different elements did you find in the previous question? Call this value q.

   (c) Compute g^{q+1}, g^{q+2} and g^{q+3}. What is your observation?

   (d) It is easy to directly compute that $21 \cdot 16 = 35 \mod 43$. Show an alternative approach to compute this, using the results from the previous sub-questions.

2. **(30 points)** The ElGamal signature scheme.

   Suppose $G = \mathbb{Z}_p$ for $p = 29$, with generator $g = 3$. For the order of G, we write $q = \varphi(p)$. In this exercise we will use the (otherwise completely insecure) hash function $H(m) = m$. Let's assume that Alice's secret key is $x = 21$. Please make sure to use the correct modulus for each step.

   (a) Determine Alice's corresponding public key y.

   (b) Sign the message $m = 15$ using ElGamal signatures with random value $r = 5$.

      i. Verify that r and q are relatively prime.

      ii. Compute $s_1 = g^r \bmod p$.

      iii. Compute $r^{-1} \bmod q$.

      iv. Compute $s_2 = (H(m) - x \cdot s_1) \cdot r^{-1} \bmod q$

   (c) Verify that the signature (s_1, s_2) is correct on message m using Alice's public key y.

      i. Check that $1 \leq s_1 < p$.

      ii. Compute $v := s_1^{s_2} \cdot y^{s_1} \bmod p$.

iii. Verify $g^{H(m)} \overset{?}{=} v$.

3. **(20 points)** Predictable randomness.

   When using the ElGamal scheme, it is crucial that one uses a fresh random number r for each use. However, true random numbers are not that easy to obtain - in practice, they are typically generated *pseudo*-randomly, and sometimes this is done poorly. When this is done in an insecure fashion, an attacker could influence the randomness, cause a system to use the same 'random' value twice or even predict the randomness completely.

   (a) Consider ElGamal encryption (let $G = \mathbb{Z}_p$ for some prime p). What can an attacker learn if the randomness r is known, and he intercepts an ElGamal ciphertext? Show how!

   (b) Now consider ElGamal signatures. Show what an attacker can learn when the randomness r is known, and he obtains an ElGamal signature (s_1, s_2) (with the corresponding message m). Again, show how!

   (c) Which of these scenarios has more devastating consequences? For example, consider the security of other ciphertexts and signatures for which the used randomness r' is still unknown.

4. **(20 points)** Bitcoin.

   The goal of this exercise is to make a Bitcoin transfer to a specific Bitcoin wallet (listed below). As was discussed during the lecture, please keep the amount small: Bitcoins are divisible to far beyond the decimal point.

   `Receiving wallet: 1Q9GTKYKamEWFVxgty48dcsJGyXjtRKyzT`

   To prove that you transferred the Bitcoin, please **send an email** to `j.rijneveld@cs.ru.nl`, mentioning the transaction ID and your student number(s).

   Hints: If you do not yet have a Bitcoin wallet, you should first create one. A simple Bitcoin wallet is the program 'Electrum' which is available for Linux, Windows, OSX and Android.

   Buying Bitcoin is easy via sites like `https://bitonic.nl`, where you can directly buy Bitcoin via iDeal transaction and have these transferred to your wallet. Unfortunately, there is a minimum transaction limit of €2.50 for this specific website. We recommend finding a group of people to make one purchase together, and then distributing fractions of the purchased Bitcoin amongst the group. Alternatively, other students might already own Bitcoin and may be willing to sell or donate a small fraction.

   From your wallet you can then make the transfer to the Bitcoin wallet mentioned above. After the transfer, you can verify whether your transfer succeeded, by searching for your transaction hash on `https://blockchain.info/`.