Cryptography I, homework sheet 8

Due: 20 November 2014, 10:45

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto14@tue.nl` or place it on the lecturer's table before the lecture. Do not email Tanja or put homework in mailboxes.

You may use computer algebra systems such as mathematica, gp, or sage or program in C, Java, or Python. Please submit your code as part of your homework. Make sure that your programs compile and run correctly; my students will not debug your programs. The program should be humanly readable.

1. The Lamport-Diffie signature scheme is called a one-time signature. Explain how and when an attacker can impersonate a user if the user happened to use a key twice (the messages are not under the control of the attacker).

2. Use factor base $\mathcal{F} = \{2, 3, 5, 7, 11, 13\}$ to solve the DLP $h = 281$, $g = 2$, in $\mathbb{F}_{1019}^*$. I.e. pick random powers of $g = 2$, check whether they factor into products of powers of 2,3,5,7,11, and 13; if so, add a relation to a matrix. The columns of the matrix correspond to the discrete logs of 2,3, 5,7,11, and 13. Once you have 6 rows try to solve the matrix; note that these computations take place modulo the group order 1018. It might be that some of the rows are linearly dependent, in that case you need to generate another relation. Once you have all discrete logs of the primes in the factor base, check whether h is smooth and if not find a h/g^i for some i which is smooth.

   E.g. $2^{291} \equiv 52 \bmod 1019$; over the integers $52 = 2^2 \cdot 13$, so we incluclude the relation $291 \equiv 2a_2 + a_{13} \bmod 1018$. Note that you can run into difficulties inverting modulo 1018 since it is not prime. E.g. $2^{658} \equiv 729 \bmod 1019$; over the integers $729 = 3^6$, so we incluclude the relation $658 \equiv 6a_3 \bmod 1018$ but 6 is not invertible modulo 1018 and we can only determine $a_3 \equiv 449 \bmod 509$ and need to test whether $a_3 = 449$ or $a_3 = 449 + 509$. Here $2^{449} \equiv 1016 \bmod 1019$ and $2^{449+509} \equiv 3 \bmod 1019$, thus $a_3 = 958$.

   Hint: if you're using Pari-GP you'll find

   ```
   factor(lift(Mod(2^i,p)))
   ```

   a usefull command.

Note that there was a typo on the board today, the solution was 97, not 91.