

Cryptography, homework sheet 4

Due: 01 October 2015, 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 the programming part to `crypto15@tue.nl` and place the written part 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 (if any) as part of your homework. If you do, make sure that your programs compile and run correctly; my students will not debug your programs. The program should also be humanly readable.

If you are a student in the old masters system and for some reason cannot substitute 2MMC10 for the course (2WC09 or 2WC12) in your study program, please contact Tanja by email. To find out whether you can substitute the course, talk to your study advisor.

1. Let $\mathbb{F}_{2^{11}}$ be represented as $\mathbb{F}_2[x]/(x^{11} + x^2 + 1)$. The element x generates a group of order 2047, so it generates the whole multiplicative group of the finite field. Solve the discrete logarithm problem $g = x, h = x^9 + x^8 + x^6 + x^4 + x^2 + x + 1$ using the Pohlig-Hellman attack and the Baby-Step Giant-Step algorithm within the two subgroups of size 23 and 89.

If you're using Pari-GP define your f using `Mod(1,2)`; then use `% f` to compute modulo f .

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

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

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

a usefull command.