Cryptography I, homework sheet 5

Due: 10 October 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. 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 `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.

For the finite field computations in $\mathbb{F}_{2^4}$ one-line answers using a computer algebra system do *not* count; you need to figure out finite fields by hand at least once. It's still a good idea to verify your answers using a computer algebra system
Please email Tanja in case you have found no way of obtaining a programmable calculator to use for the exam.

1. The integer $p = 1009$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 123$. You observe $h_a = 234$ and $h_b = 456$. What is the shared key of Alice and Bob?

2. Alice and Bob use the DH key exchange in $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4 + x + 1)$ with $g = x$. Find the order of g. Alice uses $n_A = 4$, Bob uses $n_B = 7$. Compute all parts of the key exchange, i.e. h_A, h_B and the shared key.

3. Here is a public-key system.
   Key set up. Each user does the following

   - Choose any two integers a and b.
   - Set $M = ab - 1$.
   - Choose two more integers a' and b'.
   - Set $e = a'M + a$ $d = b'M + b$, and $n = (ed - 1)/M$.

   The public key is (n, e), the secret key is d.

   Encryption: To encrypt a plaintext message m to public key (n, e) compute

   $$c \equiv em \bmod n.$$

   The owner of d can decrypt this by computing

   $$m' \equiv dc \bmod n.$$

   (a) Set up your secret key and private key starting from $a = 100, b = 103, a' = 39, b' = 51$. Decrypt $c = 42$.

   (b) Why is n an integer? Why does the system work, i.e. why is $m' = m$? Show how to obtain the secret key corresponding to the target pubic key $(118, 857)$.