Exercise sheet 6, 18 December 2014

For this exercise sheet you should not use your computer for more functions than a pocket calculator offers you (though with more digits) – unless explicitly stated.
The first six exercises are to recap finite fields and groups; skip them if you feel comfortable in that area – or just do them quickly.
The next three exercises use a bad choice of group – and you will find out why. Do not use the additive group of a finite field for DH systems!
The last exercises use a better choice – the multiplicative group of a finite field. For these small sizes you can break the system but for primes of 2048 and more bits that's beyond current computation power.

1. Write all elements of $\mathbb{Z}/13$. For each element determine the order in $(\mathbb{Z}/13, +)$. What orders do you observe; what orders could be possible?

2. Write all elements of $\mathbb{Z}/6$. For each element determine the order in $(\mathbb{Z}/6, +)$. What orders do you observe; what orders could be possible?

3. Write all elements of $(\mathbb{Z}/13)^*$. For each element determine the order in $((\mathbb{Z}/13)^*, \cdot)$. What orders do you observe; what orders could be possible?

4. Write all elements of $(\mathbb{Z}/6)^*$. For each element determine the order in $((\mathbb{Z}/6)^*, \cdot)$. What orders do you observe; what orders could be possible?

5. Show that $\mathbb{F}_{61}^* = \langle 2 \rangle$, i.e. show that the order of 2 in $\mathbb{F}_{61}$ is 60.

6. Determine the smallest generator $g \in (\mathbb{Z}/4969)^*$ that is larger than 1000. Do this by testing whether $1000+i$ is a generator, starting from $i = 1$ and incrementing i if it is not. Try to make each test as cheap as possible. For this exercise I suggest you use modular exponentiation on your computer but don't just ask it for the order.

7. The integer $p = 103$ 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 $g = 2$. You observe $h_a = 23$ and $h_b = 42$. What is the shared key of Alice and Bob?

8. The integer $p = 103$ is prime. You are the eavesdropper and know that Charlie and Dave use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 2$. You observe $h_a = 21$ and $h_b = 39$. What is the shared key of Alice and Bob?

9. The integer $p = 10007$ 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 $g = 1234$. You observe $h_a = 2345$ and $h_b = 4567$. What is the shared key of Alice and Bob?

10. This problem is about the DH key exchange. The public parameters are that the group is $(\mathbb{F}_{1009}^*, \cdot)$ and that it is generated by $g = 11$.

    (a) Compute the public key belonging to the secret key $b = 548$.

    (b) Alice's public key is $h_a = 830$. Compute the shared DH key
    with Alice using b from the previous part.

    (c) Alice and Bob keep the prime but change the generator to $g = 1008$. Simulate one round of DH key exchange. Why would you avoid this generator in practice?

11. The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. You observe $h_a = 12$ and $h_b = 14$. What is the shared key of Alice and Bob?
    It's OK if you use a brute force attack here.