Exercise sheet 4, 8 December 2016

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 exercises are about RSA so that you get some practice in breaking it. The numbers might get too big for your calculator.
The last five exercises need a short explanation of Diffie-Hellman key exchange which I will give at the beginning of the exercise session. You will see some bad choices of groups – and you will find out why these are bad. 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. Users A, B, and C are friends of S. They have public keys $(e_A, n_A) = (3, 58483), (e_B, n_B) = (3, 50629)$, and $(e_C, n_C) = (3, 54253)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 52106, c_B = 7516$, and $c_C = 4649$. What was the message?

8. For this exercise you can use your computer. Use Pollard's rho method to factor $n = 2176165112113$. Consider the update functions $z_{i+1} = z_i^2 + c$ for $c \in 3, 7, 11$ and for each case check how large i has to be so that $\gcd(S_i, n) \notin \{1, n\}$, where $S_i = (z_1 - z_2)(z_2 - z_4) \cdots (z_i - z_{2i})$, and S_i is reduced modulo n at each step.

9. For this exercise you can use your computer. Use the $p - 1$ method as on the slides with $s = \operatorname{lcm}(1, 2, 3, 4, 5, \ldots, 50)$ and base 2 to factor $n = 400428248257$. If you get stuck on the precision of your computer, remember that the exponentiation is modulo n and that you learned the square-and-multiply method to deal with large exponents. Alternatively, for the last step you can compute the exponentiation in pieces, using the factors of s.

10. For this exercise you should use a pocket calculator (or your computer with just basic functions). Use the $p-1$ method with $s = \operatorname{lcm}\{1, 2, 3, \ldots, 6\}$ and base 2 to factor $n = 101617$.

11. 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?

12. 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?

13. 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?

14. 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?

15. 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.