Cryptography Exam Mandate

Exercise 1

Consider the ring $\mathbb{Z}/1188503\mathbb{Z}$.

a) Find the order of $[4]_{1188503} \in (\mathbb{Z}/1188503\mathbb{Z})^*$.

b) How many elements of order 1008 are there in $(\mathbb{Z}/1188503\mathbb{Z})^*$?

c) Find all elements of order 6 in $(\mathbb{Z}/1188503\mathbb{Z})^*$.

Exercise 2

Consider the field $\mathbb{Z}/2\mathbb{Z}[X]/(X^4 + X + 1)$, and let $\alpha = [X]_{(X^4+X+1)}$. Determine, without the use of GAP, if α is a generator of $(\mathbb{Z}/2\mathbb{Z}[X]/(X^4 + X + 1))^*$, and find the inverse of α^8.

Exercise 3

A message m is sent to a person which encrypted using RSA with the public key (n, e), where n is the RSA-modulus and e the encryption exponent.

a) Decrypt the cipher text $c = 1516$, which was encrypted with the public key $(7153, 17)$.

b) Factorize the RSA-modulus of the public key $(139057, 7)$ using the fact that the secret key is $d = 98743$ and applying the algorithm with the number 5.

c) How many $x \in \mathbb{Z}$, with $1 < x < 139057$ and $\gcd(x, 139057) = 1$ are there such that the algorithm in the previous part finds the factor 577 at step 3 (that is when $t = 2$).

Exercise 4

The public ElGamal-key of Alice is $p = 506251$, $\alpha = 23$, and $A = 21242$.

a) The plain text is 2468, Bob takes $b = 1357$. Compute the cipher text (B, C).

b) Together with Oscar you are trying to find the secret key x of Alice using the Pohlig-Hellman Algorithm. Oscar has already established $x \equiv 1 \pmod 2$ and $x \equiv 13 \pmod{81}$. Complete the work of Oscar.

c) The cipher text is $B = 457203$, $C = 457544$. Compute the plain text.

Exercise 5

Let $A = \{a \mid a \in \mathbb{Z}, 1 \leq a < 499249, \gcd(a, 499249) = 1\}$.

a) How many $a \in A$ are there such that 499249 is an a-pseudo prime?

b) How many $a \in A$ are there such that 499249 passes the Miller-Rabin test for a with the sequence of the form $*, *, -1, 1$?

c) Find in a constructive way two $a \in A$ such that 499249 passes the Miller-Rabin test for a with the sequence $*, *, -1, 1$. You may use the fact that $[7]_{433}$ is a generator of $(\mathbb{Z}/433\mathbb{Z})^*$ and $[5]_{1153}$ is a generator of $(\mathbb{Z}/1153\mathbb{Z})^*$.

Exercise 6

Let R be a finite commutative ring with identity and $1 \neq 0$. Assume R has exactly one zero divisor. Show that $|R| = 4$ and that R is isomorphic to $\mathbb{Z}/2\mathbb{Z}[X]/(X^2)$ or $\mathbb{Z}/4\mathbb{Z}$.