Family Name .... *Name* .... *Student ID(Matricola):* ....

Solve the problems adding to the replies short and essential explenations. *Please write the solutions in the designed areas. NO EXTRA SHEETS WILL BE ACCEPTED.* 1 Problem = 4 marks. Duration: 2 hours. No questions allowed in the first hour and in the last 20 minutes.

1	2	3	4	5	6	7	8	9	TOT.

1. Answer to the following questions with a justification of one line:

   a. Is it true that if n is odd, the irreducible factors of $x^{3^n} - x$ have all odd degree?

   ....

   b. Is it true that it is not possible to elliptic curves over finite fields for the Diffie – Hellman key exchange protocol?

   ....

   c. Which is the probability that an irreducible polynomial of degree 5 over $\mathbf{F}_5$ is primitive?

   ....

   d. Is it true that there are no elliptic curves over $\mathbf{F}_{11^2}$ such that $E(\mathbf{F}_{11^2}) \cong \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/42\mathbf{Z}$?

   ....

2. After having recalled the RSA cryptosystem, decode the crypted text $\mathcal{C} = 25$ knowing tha the public key is $(7, 143)$.

3. Expain how the Miller – Rabin primality test works.

4. Explain the Goldwasser – Micali cryptosystem.

5. After having defined Carmichael numbers and having recalled their main properties, prove that 6601 is Carmichael.

6. Let $E : y^2 + \alpha y = x^3$ be and elliptic curve over $\mathbf{F}_8 = \mathbf{F}_2[\alpha], \alpha^3 = \alpha + 1$. Determine $\#E(\mathbf{F}_2[\alpha])$ and $\#E(\mathbf{F}_{2^6})$. What can be said regarding the group structure?

7. Determine the structure of group of rational points of an elliptic curve E over $\mathbf{F}_{53^2}$ knowing that it contains a point of order 392 and a unique point of order 2.

8. Consider the elliptic curve $E : y^2 = x^3 + x + 1$ and compute $\#E(\mathbf{F}_{3^{100}})$.

9. Prove that an elliptic curve defined on a field of chaacteristic 3 has at most two points of order 3.

hint: *Study the identity* $2P = -P$ *for the Weierstrass equation* $y^2 = x^3 + ax^2 + bx + c$.