

Family Name Name Student ID(Matricola):
Solve the problems adding to the replies short and essential explanations. 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	TOTAL

1. Answer the following questions providing a justification of one line:
- a. Is the Diffie-Hellmann key exchange protocol only defined for the cyclic group $\mathbf{F}_{p^n}^*$?

.....

b. Is it true that there are non-isomorphic finite fields in which the respective multiplicative groups have the same number of generators?

.....

c. If $f, g \in \mathbf{F}_p[x]$ have the same degree, is it true that the splitting field of f contains the roots of g ?

.....

d. Write down all irreducible polynomials in $\mathbf{F}_2[x]$ with degree less or equal to 4.

.....
2. After having written recursive formulas for the calculation of the Bezout identity between two integers, compute that identity for (1345, 9875). Next compute the greatest common divisor (1345, 9875) using the binary algorithm.

3. After having shown that 3 is a primitive root modulo 31, compute the discrete logarithm $\log_3 2 \in \mathbf{Z}/30\mathbf{Z}$ using the algorithm Baby Steps Giant Steps.

4. Outline some cryptographic systems that base their security on the problem of discrete logarithm .

5. Determine all integers X in the interval $[-200, 10]$ such that
$$\begin{cases} X \equiv 2 \pmod{4} \\ X \equiv 4 \pmod{5} \\ 3X \equiv 4 \pmod{7}. \end{cases}$$

6. Provide an example of explicit finite field for 32 elements and among its elements determine a primitive root.

7. Determine the degree over \mathbf{F}_{13} of the splitting field of the polynomial

$$(T^{13^8} - 27T^{13^5} + 26T^{13^4})(T^2 + 13T + 27)(T^3 + 14)(T^{13^8} + 25T^{13}) \in \mathbf{F}_{13}[T].$$

8. After having explained briefly the algorithm of successive squares, compute $\alpha^{1047} \in \mathbf{F}_7[\alpha], \alpha^3 = \alpha - 2$.