

M360 Mathematics of Information Security

homework sheet # 5

Problem # 1

If $22 = 5^x \pmod{37}$, what is x ? Use the Pohlig Hellman algorithm.

Problem # 2

On the elliptic curve over \mathbb{F}_{29} defined by $y^2 = x^3 + 4x + 20$, compute

a) $(5, 22) + (16, 27)$

b) $2 \cdot (5, 22)$

Problem # 3

a) How many points over \mathbb{F}_5 has the elliptic curve defined by $y^2 = x^3 + 3x$?

b) How many points over \mathbb{F}_5 has the elliptic curve defined by $y^2 = x^3 + 4x$?

c) Is the group of points (with respect to addition as described in the lecture) in a) cyclic?

c) Is the group in b) cyclic?

Problem # 4

Describe some properties of a projective plane which an affine plane does not have.

Problem # 5

Verify the entry (2, 8) (start counting from zero) in the Rijndael S -box. You may use the programs on the course web page to do the calculations.

Problem # 6

Find the missing digit to make the number

236_014

divisible by 66.