Dr. A. Betten Fall 2005

# M360 Mathematics of Information Security

practice exam 12/07/05

not graded!

**Exercise # 1** ( points)

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

**Exercise # 2** ( points)

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

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

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

**Exercise # 3** ( points)

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 in a) cyclic?

d) Is the group in b) cyclic?

**Exercise # 4** ( points)

Describe a few facts and properties which a projective plane has which an affine plane doesn't have.

**Exercise # 5** ( points)

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

**Exercise # 6** ( points)

Find the missing digit to make the number

236_014

divisible by 66.

**Exercise # 7** ( points)

a) Convert 712 into binary, convert $(101010111)_2$ into decimal.

b) Convert $(6651)_7$ into base 9.

**Exercise # 8** ( points)

Find the last two digits of $666^{999}$.

**Exercise # 9** ( points)

a) Find all four solutions to $x^2 \equiv 133 \bmod 153$

b) Find all two solutions to $x^2 \equiv 136 \bmod 153$

**Exercise # 10** ( points)

a) Is $X^5 + X^2 + 1$ irreducible over $\mathbb{F}_2$?

b) Is $X^5 + X + 1$ irreducible over $\mathbb{F}_2$?

**Exercise # 11** ( points)

Decipher the following affine ciphertext, using that the plaintext starts with "h" and ends with "y"

`fchmdiu`

**Exercise # 12** ( points)

Decipher the following Vigenére ciphertext, using that the key is "snow."

`wyzehgwyuhfrwfzenrwjhecfwphenrglsps`