NT-Cryptography MAT4930 *7554* **Class-Y** Prof. JLF King 1Sep2015

Y1: *Show no work. Please write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

z Prof. King wears bifocals, and cannot read small handwriting. Circle one: **True!** **Yes!** ***Who?***

a Alice's RSA code has modulus is $M = 6557$, and encryption exponent $\mathbf{E} := 749$, both public. Bob has a message that can be interpreted as a number β in $[0..M)$. Since Alice knows the secret factorization $M = p \cdot q$ into primes, p=79, q=83, she can compute the decryption exponent $\mathbf{d}$= ______ $\in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle \beta^{\mathbf{E}} \rangle_M = 007$. Alice decrypts it to $\langle \mu^{\mathbf{d}} \rangle_M =$ ______ $\in [0..M)$.

b OLD: Let $f(x) := x^2 - 4x - 2$, and $Z_0 := c_0 := 3$. Note $f(Z_0) \equiv_5 0$. Note $f'(Z_0)$= ______ $\not\equiv_5 0$. Use Hensel's lemma to compute coefficients $c_k \in [0..5)$ [*put them in the blanks, below*]

$$Z_3 = \underbrace{\overbrace{c_0 \cdot 5^0 + \_\_\_ \cdot 5^1}^{Z_1} + \_\_\_ \cdot 5^2}_{Z_2} + \_\_\_ \cdot 5^3$$

so that integers $Z_k := \sum_{i=0}^{k} c_i 5^i$ satisfy

$$f(Z_k) \equiv 0 \pmod{5^{k+1}},$$

for $k = 1, 2, 3$.

b′ Let $f(x) := x^2 - 4x - 2$, and $Z_1 := c_0 := 3$. Note $f(Z_1) \equiv_5 0$. Note $f'(Z_1) =$ ______ $\not\equiv_5 0$. Use Hensel's lemma to compute coefficients $c_k \in [0..5)$ [*put them in the blanks, below*]

$$Z_4 = \underbrace{\overbrace{c_0 \cdot 5^0 + \_\_\_ \cdot 5^1}^{Z_2} + \_\_\_ \cdot 5^2}_{Z_3} + \_\_\_ \cdot 5^3$$

so that integers $Z_k := \sum_{i \in [0..k)} c_i 5^i$ satisfy

$$f(Z_k) \equiv 0 \pmod{5^k},$$

for $k = 2, 3, 4$.

c Number $M := 229$ is prime. PoP-factor $\varphi(M)$ as ______. Compute the multiplicative-order, $\mathrm{Ord}_M(-5) =$ ______. [*Hint:* Use the Descent Alg.]

d TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is $100 \overset{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ ______.

e $S(98,000,000)$= ______ where, for posints k, let $S(k)$ be the number of mod-k square-roots of 1. BTWay, group $(\Phi(1024), \cdot, 1)$ is isomorphic to this product ______ of cyclic groups.

[Let $\mathbf{C}_N$ denote the cyclic group with N many elements.]

Y1:	___ ___ ___	195pts
Missing ORDINAL, **name** *or honor sig.*:	___ ___	−35pts
Total:	___ ___ ___	195pts