Staple!

Team:_____

NT-Cryptography MAT4930 *7554* | **Home-B** | Prof. JLF King *Touch*: 31Jul2016

BoC, Monday, 17Mar2014, Please *fill-in* every *blank* on this sheet.

B1: *Show no work. Please write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a Alice publishes her ElGamal triple: Modulus $M := 997$, base $G := 174$, and value $V := \langle G^\alpha \rangle_M = 609$, where α is her secret key. (She picks α in $[2\,..\,R)$, where $R = 498$ is the order of the subgp gen. by G.) Bob has a message $s \in [0\,..\,M)$. He picks an ephemeral $\beta \in [1\,..\,R)$, then transmits (C, D) where $C := \langle G^\beta \rangle_M = 88$ and $D := \langle s \cdot V^\beta \rangle_M = 99$. Alice knows that $\alpha = 27$, so she decodes $s =$ _____.

b The Huffman code with letter-probabilities

I:$\frac{12}{66}$ $\mathcal{M}$:$\frac{5}{66}$ O:$\frac{7}{66}$ $\mathcal{R}$:$\frac{4}{66}$ $\mathcal{S}$:$\frac{32}{66}$ $\mathcal{T}$:$\frac{6}{66}$

codes these to bitstrings: I: _____ $\mathcal{M}$: _____ O: _____ $\mathcal{R}$: _____ $\mathcal{S}$: _____ $\mathcal{T}$: _____.

Bitstring 1101101110011001110 decodes to _____, answering: "*What is Big Moose's name?*"

c So z=_____ is the smallest natnum satisfying

$$z \equiv_7 -2, \quad z \equiv_8 -1, \quad z \equiv_{11} 5, \quad z \equiv_{15} 12.$$

OYOP: *Your 2 essay(s) must be* TYPESET*, and Double or Triple spaced. Use the Print/Revise cycle to produce good, well thought out, essays. Start each essay on a* ***new*** *sheet of paper.*

Do **not** *restate the problem; just solve it.*

B2: *Magic integers* G_1=_____, G_2=_____, G_3=_____, G_4=_____, each in $[0\,..\,1260)$, are st. $g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \to \mathbb{Z}_{1260}$ is a ring-iso, where

$$g\big((z_1, z_2, z_3, z_4)\big) := \big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \big\rangle_{1260}.$$

Now consider poly $h(x) := [x+59][x-1][x+83]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 7, 4, 9, 5$, displaying the *results* in a nice table. (Do **not** show work for this step.)

Now use your ring-iso to compute *all* solns x to $h(x) \equiv_{1260} 0$, displaying the results in a table which shows *which* 4tup each came from. There are (not counting multiplicities) K:=_____ many solns. Explain your method well; then show **one** computation giving a root *different* (mod 1260) from $-59, 1, -83$.

B3: The building block of a cryptosystem uses N-*cloned* numbers, for large values of N. (Defns are below.)

i Prove: *For each positive integer* N*, that there exists an* N*-cloned number.*

ii Produce (with proof, 'natch) a 5-cloned number V=_____. (A little extra credit: Can you prove that your V is the *smallest* 5-cloned number?)

Defns. An integer **S** is ***twinned*** if it is divisible by some member of $\{4, 9, 16, 25, 36, \ldots\}$; otherwise **S** is ***twin***. (E.g $0, -8, 600$ are twinned, and $1, 130, -77$ are twin.)

For N,**S** posints, our **S** is "***N*-cloned**" if *each* member of $\{\mathbf{S} + j\}_{j=0}^{N-1}$ is twinned. E.g, **S**=8 is 2-cloned but not 3-cloned. Ditto **S**=27.

B1:	___ ___	90pts
B2:	___ ___	85pts
B3:	___ ___ ___	115pts
Not typed/double-spaced:	___ ___	−25pts
Total:	___ ___ ___	290pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: _____

Ord: _____

Ord: _____