Staple!

Team: ______

NT-Cryptography
MAT4930 *2H22*
MAT6932 *21BH*

Home-V

Prof. JLF King
Tuesday, 09Feb2016

Due: BoC, Monday, 15Feb2016, with all team-members present. *Fill-in* every *blank* on this sheet. This sheet is the *first-page* of your write-up, with your essays securely stapled to it.

V1: *Show no work. 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 $N := \varphi(100) =$ ______. So $\varphi(N) =$ ______. EFT says that $3^{1621} \equiv_N$ ______ $\in [0 .. N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are ______.

c Number $M := 6063751$ is prime. PoP-factor $\varphi(M)$ as ______. Compute the multiplicative-order, $\text{Ord}_M(157068) =$ ______. [The Descent Algorithm will be explained in class.]

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

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

V2: *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 $-59, 1, -83$.

V3: The building block of a cryptosystem uses N-*Repeating* numbers, for large values of N. (Defns are below.)

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

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

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

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

End of Home-V

V1:	___ ___ ___	110pts
V2:	___ ___	85pts
V3:	___ ___ ___	115pts
Not typed/double-spaced:	___ ___	−45pts
Total:	___ ___ ___	310pts

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: ______