Staple!

NT-Cryptography MAT4930 *7554* | **Class-A** | Prof. JLF King 2Sep2015

Please *fill-in* every *blank* on this sheet.

A3:	___ ___	70pts
A4:	___ ___	95pts
Poorly stapled, or not double-spaced:	___ ___	−15pts
Total:	___ ___ ___	165pts

Please PRINT your name and ordinal. Ta:

Ord:

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature:

A3: *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 Consider $M := p{\cdot}q = 8549$, where $p < q$ are primes. Your mole in King's organization finds out that $F := \varphi(M) = 8364$.

Then $p =$ _____ $< q =$ _____.

___ b Note $p := 137$ is prime. The (multiplicative) order of 2 mod 137 is _____.

[*Hint:* $p-1$ has very few prime factors.]

___ c Note that $\mathrm{Gcd}(15, 21, 35) = 1$. Find particular integers S, T, U so that $15S + 21T + 35U = 1$:

$S=$ _____, $T=$ _____, $U=$ _____.

[*Hint:* $\mathrm{Gcd}\big(\mathrm{Gcd}(15,21),35\big) = 1$.]

OYOP: *In grammatical English* ***sentences****, write your essay on every* ***third*** *line* (usually)*, so that I can easily write between the lines. Do* **not** *restate the question.*

A4: Abstractly describe the RSA algorithm, what is public, what private, how to compute the decryption key from the encryption key, and how to encrypt and decrypt. (Do not bother to describe LBolt, nor Repeated-squaring, but do say where they are used.)

Alice's RSA code has modulus is $M = 851$, and encryption exponent $\mathbf{E} := 317$, 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=37, q=23, 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 $\langle \mu^{\mathbf{d}} \rangle_M =$ _____ $\in [0\,..\,M)$.

End of Class-A