Staple!

Ord: ___ ___

NT-Cryptography MAT4930 *2H22* **Class-A** Prof. JLF King Wednesday 20Feb2019

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

OYOP: *In grammatical English* ***sentences****, write your essay on every* 2^{nd} *line* (usually)*, so that I can easily write between the lines.*

A5: *Show no work. Write* **DNE** *if the object does not exist or the operation cannot be performed. NB:* **DNE** $\neq \{\} \neq 0 \neq$ *Empty-word.*

___ a Prof. King thinks that submitting a ROBERT LONG PRIZE ESSAY [typically 2 prizes, $500 total] is a *really good idea.* A ten-page essay is fine. Date for the emailed-PDF is Thursday, 14March.

Circle: **Yes** **True** ***Résumé material!***

___ b Consider the three congruences C1: $z \equiv_{21} 18$, C2: $z \equiv_{15} 3$, and C3: $z \equiv_{70} 53$. Let z_j be the *smallest natnum* [or *DNE*] satisfying (C1) $\overset{\text{All}}{\therefore}$ (Cj). Then

$z_2 =$ _____ ; $z_3 =$ _____ .

___ c Modulo 187, the multiplicative-order of 87 is _____. *Hint:* Our $187 = 11{\cdot}17$, and $\varphi(187)$ has few prime factors.

___ d With $A := 29$, $B := 20$, $U := A{\cdot}B = 580$, let $\mathbf{J}$ be $(-290\,..\,290]$. There is a ring-iso $g{:}\,\mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G =$ _____ $\in \mathbf{J}$ and $H =$ _____ $\in \mathbf{J}$. A mod-U root of poly $f(x) := 20{\cdot}[x+10]^3 + 29{\cdot}[x-2]$ is $($ _____ , _____ $) \overset{g}{\mapsto$ _____ $\in \mathbf{J}$.

___ e Alice's RSA code has modulus is $N = 851$, and encryption exponent $\mathbf{E} := 317$, both public. Bob has a message that can be interpreted as a number m in $[0\,..\,N)$. Since Alice knows the secret factorization $N = p{\cdot}q$ into primes, p=23, q=37, she can compute the decryption exponent $\mathbf{d} =$ _____ $\in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle m^{\mathbf{E}} \rangle_N = 007$. Alice decrypts it to $\langle \mu^{\mathbf{d}} \rangle_N =$ _____ $\in [0\,..\,N)$.

A6: EFT says: *For each posint* N*, every integer* $\mathbf{b} \perp N$ *satisfies* $\mathbf{b}^{\varphi(N)} \equiv_N 1$.

Write a careful proof of this Euler-Fermat Thm. Recall that Φ_N is the units group of $\mathbb{Z}_N$, and $\varphi(N) := |\Phi_N|$.

You may use $\equiv$ for $\equiv_N$, and use $U := \Phi_N$.

End of Class-A

A5:	___ ___ ___	125pts
A6:	___ ___	45pts
Total:	___ ___ ___	170pts

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: _____

Jeffrey problems next col/page.

1: Jeffrey A (Joey #?) *For N and $B \geqslant 2$ positive integers,* (*Dis*)*Prove:* $\varphi(B^N - 1) \equiv_N 0$. ♢

Continuing...

2: Jeffrey B (HMMT2019.Febr) (Joey #?) *Fix prime $p > 2$ and polynomial ring $\Gamma := \mathbb{Z}_p[\![x]\!]$. Find the number of ordered-pairs (f, g) of polynomials, $f, g \in \Gamma$, satisfying*

$$g\big(f(x)\big) \overset{\text{in } \Gamma}{=\!=} x^{p^2} - x\,.$$

♢