Staple!

Ord: ___ ___

NT-Cryptography MAT4930 *0329* — **Class-U** — Prof. JLF King, Wedn., 22Feb2023

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

U5: *Show no work. Write* **DNE** *if the object does not exist or the operation cannot be performed. NB:* **DNE** $\neq \{\} \neq 0$.

___ ___ **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 Thurs., 30 Mar., 2023.

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

___ ___ **b** RSAing, Bob pubishes $N := pq$, with $p < q$ distinct primes, but foolishes writes $F := \varphi(N)$ on a napkin that Eve sees. Eve quickly computes poly $\mathsf{A}x^2 + \mathsf{B}x + \mathsf{C}$ whose roots are the hidden p and q. As formulas in N and F:

A= .... ; B= .... ; C= ....

___ ___ **c** The Huffman code with letter-weights

4: $\mathcal{H}$ 5: $\mathcal{O}$ 6: $\mathcal{A}$ 7: $\mathcal{C}$ 12: $\mathcal{E}$ 32: $\mathcal{D}$

codes these to bitstrings: $\mathcal{H}$: .... $\mathcal{O}$: ....

$\mathcal{A}$: .... $\mathcal{C}$: .... $\mathcal{E}$: .... $\mathcal{D}$: ....

Bitstring 10111010111110011111000 decodes to

.... , answering: "*What is Alice's nickname?*"

___ ___ **d** Consider the three congruences C1: $z \equiv_{15} 11$, C2: $z \equiv_{21} 5$, and C3: $z \equiv_{70} 61$. Let z_j be the *smallest natnum* [or *DNE*] satisfying (C1) $\overset{\text{All}}{\therefore}$ (Cj). Then

z_2= .... ; z_3= ....

___ ___ **e** 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 (........ , ...) $\overset{g}{\mapsto}$ .... $\in \mathbf{J}$.

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

U6: 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. Use $\mathbf{U}_N$ for the units group of $\mathbb{Z}_N$; recall $\varphi(N) := |\mathbf{U}_N|$.

You may use $\equiv$ for $\equiv_N$, and use $U := \mathbf{U}_N$.

End of Class-U

U5:	___ ___ ___	145pts
U6:	___ ___	45pts
Total:	___ ___ ___	190pts

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: ....