Staple!

Ord: __ __

NT-Cryptography
MAT4930 *0329*

Class-V

Prof. JLF King
Wedn, 29Mar2023

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

V1: *Show no work. Write* **DNE** *if the object does not exist or the operation cannot be performed. NB:* **DNE** $\neq \{\} \neq 0$.

__ __ a) Entropy $\mathcal{H}(\frac{1}{8}, \frac{1}{8}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})=$ ____________________.

__ __ b) Dictionary is 1: ε, 2: '0', 3: '00', 4: '1'. Thus EnZiv(0010000011111001) =

____

in $\langle \mathbf{7} \rangle$1 $\langle \mathbf{4} \rangle$0 ... $\boxed{\text{noise}}$ notation. In bits sent through the channel, EnZiv(0010000011) is

____.

__ __ c) "Integer 49 $\in \mathrm{QR}_{91}$" *T* *F* and "100 $\in \mathrm{QR}_{121}$" *T* *F*.

Value $K := 857$ is prime. So "$2 \in \mathrm{QR}_K$" *T* *F* and "$-8 \in \mathrm{QR}_K$" *T* *F*.

The prime decomposition of $L := 22673$ is $7{\cdot}41{\cdot}79$. So "$2 \in \mathrm{QR}_L$" *T* *F*.

__ __ d) Let $B := 625^2$. Then 507 is a B-QR: *T* *F*

__ __ e) TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is $100 \overset{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ ____________ $\in [0\,..\,250)$.

__ __ f) Modulo $Q := 72$, poly $h(x) := x^2 + 16x - 17$ has ______________ many roots. E.g, ___________ $\in [0\,..\,Q)$.

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

V2: Precisely define the Elias-δ-code; a prefix-code which maps $\mathsf{C}\colon \mathbb{Z}_+ \to \{0,1\}^+$. Prove $\dfrac{\mathrm{Len}(\mathsf{C}(n))}{L(n)} \to 1$ as $n \nearrow \infty$, where $L := \log_2$.

V1: ___ ___ ___ 145pts

V2: ___ ___ 45pts

Total: ___ ___ ___ 190pts

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

Ord:

____ __ __