Staple!

Ord: ___ ___

NT-Cryptography
MAT4930 *2H22*

Class-C

Prof. JLF King
Wedn., 10Apr2019

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

C1: *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** A *minimum* requirement for an LOR (letter-of-recommendation) from Prof. K is <u>two</u> courses. Circle:

Yes **True** **Darn tootin'!**

___ ___ **b** Entropy $\mathcal{H}(\frac{1}{16}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2})=$ ....

___ ___ **c** Dictionary is 1: ε, 2: '0', 3: '00', 4: '1'. Thus EnZiv(0010000011111001) =

....

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

....

___ ___ **d** Evaluate $Id \circledast \boldsymbol{\mu}$ on the numbers $1, 2, 5, 10, 20$:

....

Mystery function $f: \mathbb{Z}_+ \to \mathbb{Z}$ satisfies $f \circledast \boldsymbol{\tau} = Id$. So $f(20)=$ ....

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

C2: *State Shannon source-coding thm* as stated/proved in class.

C3: State *Jensen's Inequality* as a formal thm, including the IFF condition, and *defining* [not just naming] what kind of fnc $f:\mathbb{R}\to\mathbb{R}$ that *Jensen's* applies to.

Draw a LARGE, labeled picture illustrating the idea of the proof, but do not write a proof.

C4: Let $\vec{\mathbf{1}} := \texttt{1111...}$, the half-$\infty$ constant-1 bit-string. Using our Ziv-algorithm, with dictionary that [initially] only has the nullword, we start parsing $\vec{\mathbf{1}}$.

Let $P(k)$ be the largest-number of bits we've parsed, having used-up at most k many bits from $\vec{\mathbf{1}}$. I.e, we Ziv-parse, and we eventually parse a new word [which we enter into our dictionary], having read exactly $P(k)$ many bits, in total, where $P(k) \leqslant k$. As we scan for the next new word, we run past the k^{th}-bit in $\vec{\mathbf{1}}$.

i Give an approximate formula for $N(k)$, the number of words you've parsed, having read the first $P(k)$ many bits.

ii Let $Z(k)$ be the length of the Ziv-compressed bit-string that encodes the first $P(k)$ many bits in the source-string. When k is large, give a pretty good estimate for $Z(k)$; a "closed formula", neither having a $\sum$ summation operator, nor a $\prod$ product operator.

What are approximate values for $N(500,000)$, and for $Z(500,000)$?

Compute $\lim_{k\to\infty} \frac{Z(k)}{k} =$ ______.

C1:	___ ___ ___	105pts
C2:	___ ___	45pts
C3:	___ ___	50pts
C4:	___ ___	85pts
Total:	___ ___ ___	285pts

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

Ord: ______