Staple!

Ord: ___ ___

NT-Cryptography MAT4930 *2H22* | **Class-B** | Prof. JLF King Friday, 22Mar2019

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.*

B5: *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 wears bifocals, and cannot read small handwriting. Circle one: **True!** **Yes!** ***Who??***

___ b Suppose $x,y,N \in \mathbb{Z}_+$, with $x^2 + 2y^2 = N$ and $N \perp x$.
Statement "*Integer* $-2 \in \mathrm{QR}_N$" is: *AT* *AF* *Nei*
And stmt "*Integer* $+2 \in \mathrm{QR}_N$" is: *AT* *AF* *Nei*

___ c Compute a Huffman code for these five symbols.

A: 4/27 ____

B: 1/27 ____

C: 14/27 ____

D: 2/27 ____

E: 6/27 ____

When coalescing, use "0" to go to the smaller-prob. word.
And MECL($\frac{4}{27}, \frac{1}{27}, \frac{14}{27}, \frac{2}{27}, \frac{6}{27}$)= ____ bits.

___ d The Elias-delta code of posint K is

$$\mathbf{v}_K \;:=\; 0^b \; 1 \; \text{Bits}(n{+}1) \;\; \text{Bits}(K)\,,$$

where $n := |K|_{\text{Bit}}$, and $b := |n{+}1|_{\text{Bit}}$.
As $\mathbf{v}_M = 00111111011$, so $M =$ ____ .

B6: Mod $M := 145157$, note $A^2 \equiv B^2 \equiv C^2 \equiv 83521$, where $A := 289$, $B := 144868$ and $C := 17524$. These give a non-trivial factor $F :=$ ____ of M.
Explain how you computed F from A, B, C.

ii Explain where this idea might appear in the Miller-Rabin primality testing algorithm.

iii Give a formal, precise, description of the full Miller-Rabin alg.. There are several cases where M-R-Alg says "*Composite*". In each, explain the certificate of compositeness.

B7: Infinite prefix-code $\mathcal{C} = \{\mathbf{w}_1, \mathbf{w}_2, \ldots\}$ has the property that each

$$\dagger: \qquad |\mathbf{w}_K| \;\leqslant\; |K|_{\text{Bit}} + f\big(|K|_{\text{Bit}}\big)\,,$$

where $f{:}\mathbb{Z}_+ \to \mathbb{N}$. Prove that $\lim_{n\to\infty} f(n) = \infty$, using that $\mathcal{C}$ satisfies the Kraft inequality.

B5:	___ ___	90pts
B6:	___ ___	45pts
B7:	___ ___	40pts
Total:	___ ___ ___	175pts

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

Ord: ____