Staple!

NT-Cryptography MAT4930 *7554* **Class-B** Prof. JLF King 2Sep2015

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

B4: *Show no work. Please write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a The Huffman code with letter-probabilities

$\mathcal{I}{:}\frac{12}{54}$ $\mathcal{M}{:}\frac{5}{54}$ $\mathcal{O}{:}\frac{7}{54}$ $\mathcal{R}{:}\frac{3}{54}$ $\mathcal{S}{:}\frac{21}{54}$ $\mathcal{T}{:}\frac{6}{54}$

codes these to bitstrings: $\mathcal{I}$: ______ $\mathcal{M}$: ______ $\mathcal{O}$: ______ $\mathcal{R}$: ______ $\mathcal{S}$: ______ $\mathcal{T}$: ______.

Bitstring `010010111001101` decodes to ______, answering: "*What do you do to a castle?*"

b 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) $\overset{\text{All}}{\ldots}$ (Cj). Then

$z_2 =$ ______ ; $z_3 =$ ______.

c Let $f(x) := x^2 - 9x + 14$, and $N := 475 \overset{\text{note}}{=\!=} p \cdot 25$, where $p := 19$ is prime. The *number* of solns $x \in [0..N)$ to $\boxed{f(x) \equiv_N 0}$ is $K =$ ____. A number $Z \in [0..N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is ______.

[*Hint:* Find solns mod-p and mod-25, then use CRT.]

OYOP: *In grammatical English* ***sentences****, write your essays on every* ***third*** *line* (usually)*, so that I can easily write between the lines. Do* **not** *restate the question.*

B5: i *Carefully* state the ***Chinese Remainder Thm***, CRT, being precise with the hypotheses, and the conclusions. If you use a term such as "reduced-product" then carefully define it. Say what properties G_1, the first "magic number", has to have, and a give formula for G_1.

ii Define the Euler-phi fnc, φ. *Precisely* state what it means for $\varphi()$ to be a ***multiplicative-function***.

iii *Carefully* **prove** that $\varphi()$ is *multiplicative*, making precise exactly *how* and *where* you are using CRT.

B6: Part of the Kraft-McMillan Inequality Thm (K-M Thm) concerns a (binary) prefix-code with lengths $\ell_1, \ell_2, \ldots, \ell_N$. It states that

$$\left[\sum_{j=1}^{N} 1/2^{\ell_j}\right] \leqslant 1\,.$$

If this is *equality*, then the code is said to be ***complete***.

Consider a prefix-code $\mathcal{T}$ with lengths $s_1, s_2, \ldots, s_N$. Prove that there exists a prefix-code, $\mathcal{C}$, with lengths $\ell_1, \ldots, \ell_N$ that satisfy

$$*: \qquad \forall j \in [1..N]: \qquad \ell_j \leqslant s_j\,.$$

Moreover, $\mathcal{C}$ is complete.

End of Class-B

B4:	___ ___	60pts
B5:	___ ___	50pts
B6:	___ ___	40pts
Total:	___ ___ ___	150pts

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: ______