Staple!

NT-Cryptography MAT4930 *7554*

Class-W

Prof. JLF King *Touch*: 2Jul2018

W1: *Show no work. Write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

___ ___ a) Alice's RSA code has modulus is $M = 6557$, and encryption exponent $\mathbf{E} := 749$, both public. Bob has a message that can be interpreted as a number β in $[0..M)$. Since Alice knows the secret factorization $M = p \cdot q$ into primes, p=79, q=83, she can compute the decryption exponent $\mathbf{d}$= ______ $\in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle \beta^{\mathbf{E}} \rangle_M = 007$. Alice decrypts it to $\langle \mu^{\mathbf{d}} \rangle_M =$ ______ $\in [0..M)$.

___ ___ b) The Huffman code with letter-probabilities

$I{:}\frac{12}{66}$ $\mathcal{M}{:}\frac{5}{66}$ $\mathcal{O}{:}\frac{7}{66}$ $\mathcal{R}{:}\frac{4}{66}$ $\mathcal{S}{:}\frac{32}{66}$ $\mathcal{T}{:}\frac{6}{66}$

codes these to bitstrings: I: ______ $\mathcal{M}$: ______
$\mathcal{O}$: ______ $\mathcal{R}$: ______ $\mathcal{S}$: ______ $\mathcal{T}$: ______.
Bitstring 0100101110011010 decodes to ______, answering: "*How he leaves a room?*"

___ ___ c) Consider the four congruences C1: $z \equiv_{18} 15$, C2: $z \equiv_8 1$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 4$. Let z_j be the *smallest natnum* satisfying (C1) $\overset{\text{All}}{\ldots}$ (Cj). Then

z_2= ______ ; z_3= ______ ; z_4= ______.

W2: *Magic integers* G_1= ______, G_2= ______, G_3= ______, G_4= ______, each in $[0..1260)$, are st. $g{:}\mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \to \mathbb{Z}_{1260}$ is a ring-iso, where

$$g\big((z_1, z_2, z_3, z_4)\big) := \Big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \Big\rangle_{1260}.$$

Now consider poly $h(x) := [x+59][x-1][x+83]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 7, 4, 9, 5$, displaying the *results* in a nice table. (Do **not** show work for this step.)

Now use your ring-iso to compute *all* solns x to $h(x) \equiv_{1260} 0$, displaying the results in a table which shows *which* 4tup each came from. There are (not counting multiplicities) K:= ______ many solns.

Explain your method well; then show **one** computation giving a root *different* (mod 1260) from $-59, 1, -83$.

In complete English sentences OYOP, please write, double-spaced, this proof. Do **not** *restate the problem.*

W3: i) Carefully state Wilson's Thm.

ii) Carefully prove Wilson's Thm. You may use for free that a degree-n polynomial over a field has at most n roots.

End of Class-W

W1:	___ ___	90pts
W2:	___ ___	90pts
W3:	___ ___	85pts
Total:	___ ___ ___	265pts

Please PRINT your Name

______

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

Signature: ______