Staple!

Team: B

NT-Cryptography
MAT4930 *2H22*

Home-B

Prof. JLF King
Tuesday, 12Mar2019

Due: BoC, Wedn., 20Mar2019, with both team-members present. *Fill-in* every *blank* on this sheet. This sheet is the *first-page* of your write-up.

B1: *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 Consider the four congruences C1: $z \equiv_8 1$, C2: $z \equiv_{18} 15$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 3$. Let z_j be the *smallest natnum* satisfying (C1) $\overset{\text{All}}{\ldots}$ (Cj). Then

$z_2 =$ ____________ ; $z_3 =$ ____________ ; $z_4 =$ ____________ .

— — b With $K := 105$, ring $\mathbb{Z}_K$ has $|\mathrm{ZD}_K| =$ ____________ and $|\mathrm{NQR}_K| =$ ____________ .

c The Huffman code with letter-probabilities

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

codes these to bitstrings: $\mathcal{I}$: ⌞. . . . .⌟ $\mathcal{M}$: ⌞. . . . .⌟
$\mathcal{O}$: ⌞. . . . .⌟ $\mathcal{R}$: ⌞. . . . .⌟ $\mathcal{S}$: ⌞. . . . .⌟ $\mathcal{T}$: ⌞. . . . .⌟.
Bitstring 1101101110011001110 decodes to
⌞. . . . .⌟, answering: "*What is Big Moose's name?*"

B2: *Produce an infinite prefix-code* $\mathcal{C} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots\}$ *such that* $\lim_{K\to\infty} \frac{|\mathbf{v}_K|}{|K|_{\text{Bit}}} = 1.$

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

Ord:
⌞. . . . .⌟⌞.⌟⌞.⌟

Ord:
⌞. . . . .⌟⌞.⌟⌞.⌟

B3: *Magic integers* $G_1 = \underline{\qquad\qquad}$, $G_2 = \underline{\qquad\qquad}$, $G_3 = \underline{\qquad\qquad}$, $G_4 = \underline{\qquad\qquad}$, 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

$$g\big((z_1,z_2,z_3,z_4)\big) := \Big\langle z_1G_1+z_2G_2+z_3G_3+z_4G_4\Big\rangle_{1260}.$$

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 $\boxed{h(x)\equiv_{1260} 0}$, displaying the results in a table which shows *which* 4tup each came from. There are (not counting multiplicities) $K := \underline{\qquad\qquad\qquad\qquad\qquad}$ many solns. Explain your method well; then show **one** computation giving a root *different* (mod 1260) from -59, 1, -83.

B4: Alice used 32-symbol alphabet "abc...z '.?!," mapped to $[0..32)$. She sent this 31-character phrase

"lz'pslpjp!r.prphls?pjspvzp!?rsq"

about her feelings at the end of the semester. So, likely, the cleartext starts with a word expressing distress: "Alas!", "Woe!", "Oy vey!", or some such, and probably ends with punctuation. (My mole in Alice's organization suggests the word "code" is in her message.) The encryption affine-map is thus $\alpha \mapsto \Big[[\,\underline{\qquad}\cdot\alpha] + \underline{\qquad}\Big]$ mod-32. Decryption is $\beta \mapsto \Big[[\,\underline{\qquad}\cdot\beta] + \underline{\qquad}\Big]$ mod-32. The full cleartext is

$\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$

$\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$

End of Home-B

B1:	___ ___	95pts
B2:	___ ___ ___	115pts
B3:	___ ___	95pts
B4:	___ ___	45pts
Total:	___ ___ ___	350pts