



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)  $\wedge \dots \wedge$  (Cj). Then

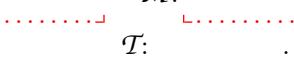
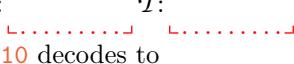
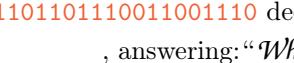
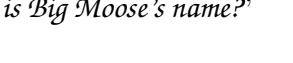
$$z_2 = \dots ; z_3 = \dots ; z_4 = \dots .$$

**b** With  $K := 105$ , ring  $\mathbb{Z}_K$  has  $|\mathbb{Z}_K^*| = \dots$  and  $|\text{NQR}_K| = \dots$

c

The Huffman code with letter-probabilities

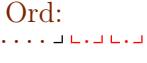
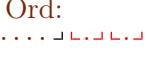
$$I: \frac{12}{66} \quad \mathcal{M}: \frac{5}{66} \quad O: \frac{7}{66} \quad \mathcal{R}: \frac{4}{66} \quad \mathcal{S}: \frac{32}{66} \quad \mathcal{T}: \frac{6}{66}$$

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

**B2:** Produce an infinite prefix-code  $\mathcal{C} = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \dots\}$

such that  $\lim_{K \rightarrow \infty} \frac{|\mathbf{v}_K|}{|K|_{\text{Bit}}} = 1$ .

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

Ord:   
 Ord: 

**B3:** Magic integers  $G_1 = \dots$ ,  $G_2 = \dots$ ,  
 $G_3 = \dots$ ,  $G_4 = \dots$ , each in  $[0..1260]$ ,  
 are st.  $g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_{1260}$  is a ring-iso, where

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

Consider  $\text{poly } h(x) := [x + 59][x - 1][x + 83]$ . 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* 4tuple 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.

**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  $\alpha \mapsto \left[ \begin{bmatrix} \cdot & \cdot \\ \text{L} & \dots & \text{L} \end{bmatrix} \cdot \alpha \right] + \left[ \begin{bmatrix} \cdot \\ \text{L} & \dots & \text{L} \end{bmatrix} \right]$  mod-32. Decryption is  $\beta \mapsto \left[ \begin{bmatrix} \cdot & \cdot \\ \text{L} & \dots & \text{L} \end{bmatrix} \cdot \beta \right] + \left[ \begin{bmatrix} \cdot \\ \text{L} & \dots & \text{L} \end{bmatrix} \right]$  mod-32. The full cleartext is

.....

End of Home B

B1: 95pts

**B2:** 115pts

**B3:** 95pts

**B4:** 45pts

**Total:** 350pts