

NT-Cryptography  
MAT4930 7554

**Project-Y**

Prof. JLF King  
Touch: 6May2016

**Y1:** Alice used 32-symbol alphabet “abc...z ’.?!,” mapped to [0..32). She sent this 31-character phrase

“lz’pslpjp!r.prphls?pjpsvpzpf!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  $\alpha \mapsto \left[ \left[ \text{.....} \cdot \alpha \right] + \text{.....} \right] \text{mod-32}$ . Decryption is  $\beta \mapsto \left[ \left[ \text{.....} \cdot \beta \right] + \text{.....} \right] \text{mod-32}$ . The full cleartext is

.....  
.....

OYOP: *Your 2 essay(s) must be TYPESET, and Double or Triple spaced. Use the Print/Revise cycle to produce good, well thought out, essays. Start each essay on a NEW sheet of paper.*

Do not restate the problem; just solve it.

**Y2:** Your goal is to prove:

†: **The Sixteen Thm.** For each oddprime  $p$ , the congruence  $x^8 \equiv_p 16$  admits a solution.

In your WU, you may use  $\sim$  for  $\equiv_4$  and  $\approx$  for  $\equiv_8$ , if you wish. But use  $\equiv_p$  or  $\equiv$  for congr-mod- $p$ .

**α** FTSOC, suppose you have a  $p$  with no solution to  $x^8 \equiv_p 16$ . Prove that  $2 \in \text{NQR}_p$  and  $-1 \in \text{QR}_p$ . Use LSThm to compute  $\langle p \rangle_8$  as a non-negative residue.

**β** Let  $r$  be a  $p$ -sqrt of -1. Use LST to prove that  $r \in \text{QR}_p$ . But use a different part of LST to prove that  $r \in \text{NQR}_p$ . Contradiction, QED.

**γ** Give an example of a 2 digit prime  $q :=$  ..... with  $2 \in \text{NQR}_q$  and  $-1 \in \text{QR}_q$ . Using symmetric residues,  $\text{QR}_q = \{ \text{.....} \}$  and  $\text{NQR}_q = \{ \text{.....} \}$ . Finally,  $[ \text{.....} ]^8 \equiv_q 16$ .

Give an example of a 3 digit prime  $p :=$  ..... with  $2 \in \text{NQR}_p$ , and values  $r :=$  ..... and  $s :=$  ..... satisfying  $r^2 \equiv_p -1$  and  $s^2 \equiv_p r$ .

**Y3:** The building block of a cryptosystem uses  $N$ -boxy numbers, for large values of  $N$ . (Defns are below.)

**i** Prove: For each positive integer  $N$ , that there exists an  $N$ -boxy number.

**ii** Produce (with proof, 'natch) a 5-boxy number  $V =$  ..... (A little extra credit: Can you prove that your  $V$  is the *smallest* 5-boxy number?)

**Defns.** An integer  $S$  is *squarish* if it is divisible by some member of  $\{4, 9, 16, 25, 36, \dots\}$ ; otherwise  $S$  is *square-free*. (E.g 0, -8, 600 are squarish, and 1, 130, -77 are square-free.)

For  $N, S$  posints, our  $S$  is “ $N$ -boxy” if *each* member of  $\{S + j\}_{j=0}^{N-1}$  is squarish. E.g,  $S=8$  is 2-boxy but not 3-boxy. Ditto  $S=27$ .

End of Project-Y

**Note.** The project is due by **noon, on Friday, 26Apr2013**, slid completely under my office door. Thank you.

<b>Y1:</b>	_____	25pts
<b>Y2:</b>	_____	125pts
<b>Y3:</b>	_____	95pts
Not typed/double-spaced:	_____	-15pts

**Total:** \_\_\_\_\_ 245pts

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: \_\_\_\_\_