Staple!

Ord: ___ ___

NT-Cryptography MAT4930 *7554* | **Project-Y** | Prof. JLF King *Touch*: 2Jul2018

Y1: 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 $\alpha \mapsto \left[\left[\quad\cdot\alpha\right]+\quad\right]$ mod-32. Decryption is $\beta \mapsto \left[\left[\quad\cdot\beta\right]+\quad\right]$ mod-32. The full cleartext is

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

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 $2 \in \mathrm{NQR}_p$ and $-1 \in \mathrm{QR}_p$. Use LSThm to compute $\langle p\rangle_8$ as a non-negative residue.

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

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

Give an example of a 3 digit prime $p :=$ with $2 \in \mathrm{NQR}_p$, 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 $\{4, 9, 16, 25, 36, \ldots\}$; 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 $\{\mathbf{S}+j\}_{j=0}^{N-1}$ 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.

Y1:	___ ___	25pts
Y2:	___ ___ ___	125pts
Y3:	___ ___	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: