Staple!

Ord: ___ ___

NT-Cryptography
MAT4930 *2H22*
MAT6932 *21BH*

Class-W

Prof. JLF King
Wednesday, 17Feb2016

Please *fill-in* every *blank* on this sheet.

W5: *Show no work. Please write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a Alice used 32-symbol alphabet "`abc...z '.?!,`" mapped to $[0\,..\,32)$. She sent this 29-character phrase

"`lzpy?z'pslpjp!r.prp!?rsphls?q`"

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

b Fix a prime q and natnums J and R. Then a closed-formula for σ_J is: $\sigma_J(q^R) =$.

Apply the [correct] CF; leave your answer as a product: $\sigma_2(980) =$

OYOP: *In grammatical English* **sentences**, *write your essay on every* **third** *line* (usually), *so that I can easily write between the lines. Do* **not** *restate the question.*

W6: i Carefully state the Quadratic-reciprocity Thm.

ii Give an example where the Legendre-symbols (LSes) are equal, computing the LSes.

Give an example where the LSes are differ, again with computation.

W7: ω Define ***Jacobi-symbol*** $\left[\frac{T}{B}\right]$, first saying precisely what kind of thing T is and B is. Now *carefully* define $\left[\frac{T}{B}\right]$.

α Describe the Jacobi-symbol "LBolt-ish" algorithm.

β Show the computation of Jacobi $\left[\frac{328}{899}\right] =$ in a nice table, giving the reason for each negation of the jacobi-register.

End of Class-W

W5:	___ ___	65pts
W6:	___ ___	45pts
W7:	___ ___	45pts
Total:	___ ___ ___	155pts

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: