Staple!

Ord: ___ ___

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

Home-W

Prof. JLF King
Wedn, 23Mar2016

Due: BoC, Wednesday, 30Mar2016. *Fill-in* every *blank* on this sheet. This sheet is the *first-page* of your write-up, with your essays securely stapled to it.

W1: *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 Using 32-symbol alphabet "`abc...z '.?!,`" mapped to $[0\,..\,32)$, the 36-character phrase

"`bpqzinpngbfypjnx!p,ujx!pbqqzufb zan'`"

comes from cleartext which *undoubtedly* starts with "`a fine`". 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 $S(98,000,000)=$ where, for posints k, let $S(k)$ be the number of mod-k square-roots of 1. BTWay, group $\big(\Phi(1024),\cdot,1\big)$ is isomorphic to this product of cyclic groups.
[Let $\mathbf{C}_N$ denote the cyclic group with N many elements.]

OYOP: *Your 3 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.*

W2: i Use Pollard-ρ to find a non-trivial factor of $M := 557489183$, using seed $s_0 := 1$ and map $f(x) := 1+x^2$. Make a nice table, labeled

Time	Tortoise	Hare	$s_{2k} - s_k$	Gcd(??)

—*but* ***replace*** *the "??" with the correct expression.* You found non-trivial factor $E :=$.
The hare Hits into the tortoise at time $H :=$.

Repeat, showing the table for $s_0 := 7$. Experiment with different seeds; what is the typical running time? How is it related to the factor you find?

ii A seed s determines a ***tail***; the smallest natnum T for which there is a time $n > T$ with $f^n(s) = f^T(s)$. The smallest such n is $T+L$ where L is the ***period***. Derive (picture+reasoning) a formula for the hitting time $H(T,L)$. [*Hint:* $H(0,L) = L$.]

iii Produce a Floyd-done-twice algorithm that computes both T and L. The number, N, of f-evaluations is upper-bounded by some small constant times $T+L$ (=arclength of ρ). How small can you get $N(T,L)$? [*Hint:* $N(0,L) = 3L$.]

W3: Suppose the letters `A F H M N U` have frequencies $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$, respectively. Construct the unique Huffman prefix-code with these frequencies; at each coalescing, use `0` for the less-probable branch and `1` for the more-probable. **Draw** the Huffman tree (large!). Label the branches and leaves with bits and letters. The name `HUFFMAN` encodes to .
Examining the tree, what kind of *Being* is `HUFFMAN`?
Answering the question *"What're y'all?"*, message `10100010101001110100110111010`*!* decodes to *!*

W4: [See (1.1) and (1.1′) in our "Notes on Codes"]. Over some alphabet $\mathbf{G}$ of cardinality $\Gamma := |\mathbf{G}|$, ***either:*** Produce a code $\mathcal{C}$ which is *weakly-UD* but not *UD*; ***or*** prove that no such code exists.

End of Home-W

W1:	___ ___	90pts
W2:	___ ___ ___	115pts
W3:	___ ___	55pts
W4:	___ ___	55pts
Total:	___ ___ ___	315pts

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:

Ord: