Staple!

NT-Cryptography MAT4930 *7554* | **Home-E** | Prof. JLF King *Touch*: 2Jul2018

Due no-later-than: noon, Monday, 28Apr2014 slid *completely* under my office door, LITTLE HALL 402 [top floor, north-east corner.] Then please *email me* that you have handed-in a project.

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.*

E1:

α For $k \in \mathbb{Z}_+$, let $J_k := \text{Lcm}(1, 2, 3, \ldots, k)$. Describe, with proof, those $k \geqslant 2$ s.t $J_k \neq J_{k-1}$. Since $J_{15} = 360360$, necessarily $J_{16} =$ _____.

β Find a factor of $N := 152557$, via "Pollard $p-1$" applied to seed $:= 3$, as follows. Note that

$$s_{15} := \langle 3^{J_{15}} \rangle_N \equiv 60339\,.$$

Compute $s_{16}, s_{17}, \ldots$ and $\text{Gcd}([s_k]-1, N)$ until you find a nt-factor, call it $F=$ _____, found at time $T=$ _____. Display the results in a nice table.

γ *Explain* how this algorithm works. What are the other factors of N? *Explain* why F was found before they were. *Explain* precisely how T is related to (factors of some number related to) F.

E2: i Use Pollard-ρ to find a non-trivial factor of $M := 59749$, using seed $s_0 := 7$ 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 $s_0 := 24$. 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:* $N(0, L) = 3L$.]

E3: Create an *interesting*, non-trivial problem involving codes, then solve it. I will judge partly on your creativity.

E1:	___ ___	95pts
E2:	___ ___	95pts
E3:	___ ___	35pts
Total:	___ ___ ___	225pts

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: _____

Folks, I have had a great time working with you this Semester. Stop by next semester to "Talk Math".

Cheers, Prof. Sieve-brain