Staple!

Team X____

NT-Cryptography MAT4930 *7554* — **Home-X** — Prof. JLF King, *Touch*: 2Jul2018

This take-home is due at the BoC of **Mon, 21Mar2011**. Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed. Fill-in *all* blanks *on this sheet*! (*Handwriting is fine; don't bother to type*).

For essay questions (X1) *and* (X2), *carefully typeset* (TEX/LATEX is recommended) *a double-or-triple–spaced essay solving the problem.* *Do not* *re-state the problem! Please start each essay on a new sheet of paper.*

X1: We work modulo $M := 191$, which is prime. Its multiplicative-group, Γ, has $\varphi(191)=190$ elements. This Γ is cyclic, and $G := 19$ is a generator, i.e $\text{Ord}_\Gamma(G) = 190$.

Use BSGS ("Baby-Step Giant-Step") to compute the unique exponent E in $[0..190)$ for which

$$19^E \equiv_M 23\,.$$

__ __ **a** Draw a large circle-picture and label the entries of the bottom-right patch by $G^0 \equiv 1$, $G^1 \equiv 19$, $G^2 \equiv 170$, ... up to $G^{12} \equiv ??$, putting in the actual values. [*Optional:* Produce a sorted version of this list, for binary searching.]

__ __ **b** Draw in the other patches; how many are there? By how much does our last patch overlap our initial patch?

__ __ **c** What is the value of the multiplier, call it U, which carries us back to the previous patch? Now use BSGS to compute the above E. Which patch was it in?

__ __ **d** Use repeated-squaring to check that your value for E is correct.

X2: **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

$$\text{Time}\,\big|\,\text{Tortoise}\,\big|\,\text{Hare}\,\big|\,s_{2k}-s_k\,\big|\,\text{Gcd}(??)$$

—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:* $N(0,L) = 3L$.]

X3: Show no work.

a Let $f(x) := x^2 - 9x + 14$, and $N := 30425 \overset{\text{note}}{=\!=} \mathsf{p}\cdot 25$, where $\mathsf{p} := 1217$ is prime. The *number* of solns $x \in [0..N)$ to $f(x) \equiv_N 0$ is $K=$ _____. A number $Z \in [0..N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is _______________.

[*Hint:* Find solns mod-p and mod-25, then use CRT.]

b Note $\mathsf{p} := 137$ is prime. The (multiplicative) order of 2 mod 137 is ______________.

[*Hint:* $\mathsf{p}-1$ has very few prime factors.]

End of Home-X

X1:	__ __ __	135pts
X2:	__ __ __	135pts
Poorly stapled, **X3:**	__ __	45pts
or missing names or team number:	__ __	−15pts
Not double-spaced:	__ __	−15pts
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: ____ __ __