Staple!

Team X_____

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

X1: *Show no work. Write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

___ a $S(98,000,000)=$ ____ where, for posints k, let $S(k)$ be the number of mod-k square-roots of 1. BTWay, group $(\Phi(1024),\cdot,1)$ is isomorphic to this product ____ of cyclic groups. [Let $\mathbf{C}(N)$ denote the cyclic group with N many elements.]

___ b $N := \varphi(100)=$ ____. So $\varphi(N)=$ ____. EFT says that $3^{1621} \equiv_N$ ____ $\in [0\,..\,N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are ____.

___ c Modulo 309, the multiplicative-order of 5 is ____. [*Hint:* $\varphi(309)$ has very few prime factors.]

___ d Three Jacobi symbols: Two blanks are immed.: $\left(\frac{51}{289}\right)=$ ____. $\left(\frac{-353}{902491}\right)=$ ____. $\left(\frac{7554}{4930}\right)=$ ____.

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.*

X2: As polynomials in $\Gamma := \mathbb{Z}_7[x]$, let

$$B(x) := x^4 - 2x^3 + x - 2\,;$$
$$C(x) := x^3 + 3x^2 - 3x\,.$$

Write t.fol polys, using coeffs in [-3 .. 3]; use $\equiv$ for equality in $\mathbb{Z}_7$ and in Γ. Compute quotient and remainder polys, $q(x) \equiv$ ____ & $r(x) \equiv$ ____, with $B \equiv [q \cdot C] + r$ and $\mathrm{Deg}(r) < \mathrm{Deg}(C)$.

Let $D := \mathrm{Gcd}(B,C)$. **Monic** $D(x) \equiv$ ____.

Compute polys $S(x) \equiv$ ____, $T(x) \equiv$ ____ st. $[S \cdot B] + [T \cdot C] \equiv D$.

X3: 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:* $N(0,L) = 3L$.]

End of Home-X

X1:	___ ___ ___	110pts
X2:	___ ___	90pts
Poorly stapled, or missing names or Honor code: **X3:**	___ ___ ___	125pts
	___ ___	−15pts
Not typed/double-spaced:	___ ___	−15pts
Total:	___ ___ ___	325pts

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: ____