Staple!

Team A

NT-Cryptography MAT4930 *7554* | **Home-A** | Prof. JLF King *Touch*: 4Aug2016

BoC, Monday, 10Feb2014, Please *fill-in* every *blank* on this sheet.

A1: *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 $N := \varphi(100) =$. So $\varphi(N) =$. EFT says that $3^{1621} \equiv_N$ $\in [0\,..\,N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are .

b Number $M := 229$ is prime. PoP-factor $\varphi(M)$ as . Compute the multiplicative-order, $\text{Ord}_M(-5) =$. [*Hint:* Use the Descent Alg.]

c 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 $\text{Deg}(r) < \text{Deg}(C)$.

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

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

OYOP: *Your 2 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.*

A2: Consider $M := p{\cdot}q = 40349$, where $p < q$ are primes. Your mole in King's organization finds out that $F := \varphi(M) = 39936$. Use the method from class, showing all the steps, to compute the factors $p =$ $< q =$.

A3: The RSA system uses a modulus $M := p{\cdot}q$, where $p < q$ are primes. A message in an element of $\mathbb{Z}_M$. In class, we required this elt be coprime to M, but this is not necessary. So: In our text, solve [prove] problem **3.2**, on P.176. It refers to Proposition 3.4, on P.116.

End of Home-A

A1:	___ ___	80pts
A2:	___ ___	80pts
Poorly stapled, or missing names or Honor code: **A3:**	___ ___ ___	105pts
	___ ___	−15pts
Not typed/double-spaced:	___ ___	−25pts
Total:	___ ___ ___	265pts

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: