

NT-Cryptography
MAT4930 7554

Home-A

Prof. JLF King
Touch: 2Jul2018

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

A1: Show no work. Write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

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

b Number $M := 229$ is prime. PoP-factor $\varphi(M)$ as $\underline{\dots\dots\dots}$. Compute the multiplicative-order, $\text{Ord}_M(-5) = \underline{\dots\dots\dots}$. [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,
 $q(x) \equiv \underline{\dots\dots\dots}$ & $r(x) \equiv \underline{\dots\dots\dots}$,
 with $B \equiv [q \cdot C] + r$ and $\text{Deg}(r) < \text{Deg}(C)$.
 Let $D := \text{Gcd}(B, C)$. Monic $D(x) \equiv \underline{\dots\dots\dots}$.

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

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.

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

$p = \underline{\dots\dots\dots} < q = \underline{\dots\dots\dots}$.

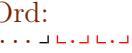
A3: The RSA system uses a modulus $M := p \cdot q$, where $p < q$ are primes. A message in an element of \mathbb{Z}_M . In class, we required this elt be coprime to M , but this is not necessary. So: In our text, solve [prove] problem 3.2, on P.176. It refers to Proposition 3.4, on P.116.

End of Home-A

A1:	<u>.....</u>	80pts
A2:	<u>.....</u>	80pts
Poorly stapled, or missing names or Honor code:	<u>.....</u>	105pts
Not typed/double-spaced:	<u>.....</u>	-15pts
	<u>.....</u>	-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: 
..... 
..... 