NT-Cryptography
MAT4930 *7554*

Class-X

Prof. JLF King
31Aug2015

X4: *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 Three Jacobi symbols: Two blanks are immed.: $\left(\frac{1531}{731}\right)=$ .... $\left(\frac{-321}{936}\right)=$ .... $\left(\frac{133}{437}\right)=$ ....

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

c Applying the Floyd cycle-finding (Tortoise & Hare) to a finite orbit which has tail $T := 7$ and eventual-period $L := 9$, yields *hitting time* $H=$ ....

d Using dictionary 0: ε, 1: "1", 2: "0", compute EnZiv(11110110)= .... , in $\langle\mathbf{7}\rangle$1$\langle\mathbf{34}\rangle$0... notation. In bits, EnZiv(11110110) is

....

e Poly $Q(x) := x^4 - 12x^3 - 8x^2 - 19x + 437$ factors completely mod 13 as:

$\left\langle Q(x)\right\rangle_{13} =$ ....

OYOP, show the following table.

X5: Use Pollard-ρ to find a non-trivial factor of $N := 110057$, using seed $s_0 := 5$ 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 $E :=$ ....

[*Fact:* Your table has $\leqslant$6 lines.]

End of Class-X

X4:	___ ___ ___	105pts
X5:	___ ___	70pts
Total:	___ ___ ___	175pts