Staple!

Team W____

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

This take-home is due at the BoC of **Wedn, 16Feb2011**. 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 (W1) *and* (W2), *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.*

W1: The building block of a cryptosystem uses N-*boxy* numbers, for large values of N. (Defns are below.)

i Prove: *For each positive integer N, that there exists an N-boxy number.*

ii Produce (with proof, 'natch) a 5-boxy number V= ______. (A little extra credit: Can you prove that your V is the *smallest* 5-boxy number?)

Defns. An integer **S** is ***squarish*** if it is divisible by some member of $\{4, 9, 16, 25, 36, \ldots\}$; otherwise **S** is ***square-free***. (E.g 0, -8, 600 are squarish, and 1, 130, -77 are square-free.)

For N,**S** posints, our **S** is "***N-boxy***" if *each* member of $\{\mathbf{S}+j\}_{j=0}^{N-1}$ is squarish. E.g, **S**=8 is 2-boxy but not 3-boxy. Ditto **S**=27.

W2: Suppose the letters `A F H M N U` have frequencies $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$, respectively. Construct the unique Huffman prefix-code with these frequencies; at each coalescing, use 0 for the less-probable branch and 1 for the more-probable. **Draw** the Huffman tree (large!). Label the branches and leaves with bits and letters. The name `HUFFMAN` encodes to

______________________________.

Examining the tree, what kind of *Being* is `HUFFMAN`?

Answering the question "*What're y'all?*", message `101000101010011101001101110 10`*!* decodes to ______________________________*!*

W3: Show no work.

a Sequence $\vec{\mathbf{s}} := (s_n)_{n=-\infty}^{\infty}$ is defined by recurrence

$$s_{n+2} = 2s_{n+1} + 3s_n,$$ with initial-conditions $s_1 := -1$ and $s_0 := 7$.

With $\mathbf{v}_n := \begin{bmatrix} s_{n+1} \\ s_n \end{bmatrix}$, matrix M := ______ satisfies $\forall k$: $\mathbf{v}_k = \mathsf{M}^k \mathbf{v}_0$. Henceforth in ring $\mathbb{Z}_{100} = [0..100)$, power $\mathsf{M}^{512} \equiv$ ______ and $s_{833} \equiv$ ______.

b Let $\boldsymbol{\tau}()$ and $\boldsymbol{\sigma}()$ be the number-of and sum-of divisors, resp.. Then $\boldsymbol{\tau}(2700) =$ ______ and $\boldsymbol{\sigma}(2700) =$ ______. (Please leave each answer as a product of three integers.)

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 $\mathrm{Deg}(r) < \mathrm{Deg}(C)$.

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

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

End of Home-W

W1:	___ ___ ___	140pts
W2:	___ ___	85pts
W3:	___ ___	75pts
Poorly stapled, or missing names or team number:	___ ___	−15pts
Not double-spaced:	___ ___	−15pts
Total:	___ ___ ___	300pts

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: ____