NT-Cryptography
MAT4930 2H22
Home-W
Prof. JLF King
Wedn. 23Mar2016

Due: BoC, Wednesday, 30Mar2016. Fill-in every blank on this sheet. This sheet is the first-page of your write-up, with your essays securely stapled to it.

W1: Show no work. Write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

Using 32-symbol alphabet “abc...z’,?!” mapped to [0..32], the 36-character phrase “bpqzinpgfbypjnx!p,u¡x!pbqqzufb zan’” comes from cleartext which undoubtedly starts with “a fine”. The encryption affine-map is thus 
\[ \alpha \mapsto \left[ \begin{array}{c} s \alpha + \beta \end{array} \right] \mod 32. \] Decryption is 
\[ \beta \mapsto \left[ \begin{array}{c} s \beta + \alpha \end{array} \right] \mod 32. \] The full cleartext is “starts with “a fine”.

\[ S(98,000,000) = \] 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 \( C(N) \) denote the cyclic group with \( N \) many elements.]

OYOP: Your 3 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.

W2: Use Pollard-\( \rho \) to find a non-trivial factor of \( M := 557489183 \), using seed \( s_0 := 1 \) and map \( f(x) := 1 + x^2 \). Make a nice table, labeled

<table>
<thead>
<tr>
<th>Time</th>
<th>Tortoise</th>
<th>Hare</th>
<th>( s_{2k} - s_k )</th>
<th>( \gcd(??) )</th>
</tr>
</thead>
</table>

—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 \( s_0 := 7 \). Experiment with different seeds; what is the typical running time? How is it related to the factor you find?

A seed \( s \) determines a \textbf{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 \textbf{period}. Derive (picture-reasoning) a formula for the hitting time \( H(T, L) \).

[Hint: \( H(0, L) = L \)]

W3: Suppose the letters A F H M N U have frequencies \( \frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{41}{170}, \frac{41}{170} \), 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. \textbf{Draw} the Huffman tree (large!). Label the branches and leaves with bits and letters. The name \textbf{HUFFMAN} encodes to

Examining the tree, what kind of \textbf{Being} is \textbf{HUFFMAN}?

Answering the question “What’re y’all?”

message \textbf{1010001010101110100110111010} decodes to...

W4: [See (1.1) and (1.1') in our “Notes on Codes”]. Over some alphabet \( G \) of cardinality \( \Gamma := |G| \), \textbf{either}: Produce a code \( C \) which is \textbf{weakly-UD} but \textbf{not UD}; \textbf{or} prove that no such code exists.

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