

## Info For Midterm

*Topics that may be on the midterm:*

1. **Boolean Formulas**  $\wedge$ ,  $\vee$ ,  $\neg$ , Formulas, Truth Tables, Circuits.
2. **Quantifiers**  $(\exists)$ ,  $(\forall)$ , finding domains to make statements true, finding domains to make statements false.
3. **Mods** Computing with mods, repeated squaring, using Euler's theorem to do exponentiation (That's the theorem  $a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}$ ). Finding inverses mod  $p$ .
4. **Crypto** Shift, Affine, General Sub (that is when you permute  $a, b, c, \dots, z$  at random), Vigenere, Matrix (don't worry, you won't have to invert a matrix). Both how to encode, how to decode, and how to break.

*Topics that WILL NOT be on the midterm:*

1. The Combinatorics that Yo has been doing in recitation. (It may be integrated into the material later and be tested on later.)
2. Intermediary Truth Values, Truth Tellers and Normals, Duplicator-Spoiler Games.

*Advice*

1. Make sure you understand the Solutions to the HW.
2. Make sure you understand the Solutions to the quizzes (the questions that are not combinatorics).
3. What is covered in class is your best guide to what I care about and may ask about.
4. If I have notes or slides on line relevant to the material, then read those.

*Nuts and Bolts*

1. The exam is Wed March 4, 6:00PM-8:00PM in CSI 3117 (the big room on the third floor). You will get every other seat.
2. If you have a class until 6:30 (some of you have told me this) then you can get there by 7:00 and take it 7:00-9:00
3. You may bring a sheet of notes, 8.5 by 11, both sides. You can write whatever you want on it. See later about advice about the sheet.

*Advice on the Sheet*

1. Making it up may be more helpful than the sheet itself.
2. Trying to cram everything you know into the sheet with really small fonts never really works.
3. Trying to copy an answer from your sheet onto the exam never really works. I did a blog post on that a while back which is on the course website.