Math/CS 103 Professor: Padraic Bartlett

Homework 15: Cryptography (Modern)

Due Friday, week 9 *UCSB 2014*

Homework Problems.

Pick **three** of the following **five** problems to solve!

1. Prove Fermat's Little Theorem:

   Theorem 1. *Let p be a prime number. Take any $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Then*

   $$a^{p-1} \equiv 1 \mod p.$$

2. A **group** is the following object: a set G along with an operation $\cdot$ that satisfies the following properties:

   - **Associativity**: For all a, b and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
   - **Identity element**: There exists an element e in G such that for all a in G, $e \cdot a = a \cdot e = a$.
   - **Inverse element**: For each a in G, there is an element b in G such that $a \cdot b = b \cdot a = e$, where e is an identity element.

   (a) Show that $\mathbb{Z}/n\mathbb{Z}$ is a group, if we let the group operation be defined as addition mod n.

   (b) Show that $\mathbb{Z}/n\mathbb{Z}$ is **not** a group, if we let the group operation be defined as multiplication mod n.

   (c) Let $(\mathbb{Z}/n\mathbb{Z})^{\times}$ denote the set of numbers $\{1, \ldots n-1\}$. Show that this is a group precisely whenever n is a prime number, if we let the group operation be defined as multiplication mod n.

3. Let G be a group with group operation $\cdot$ and identity element e. For any a in this group, let a^k denote the object $\overbrace{a \cdot a \cdot \ldots \cdot a}^{k \text{ times}}$. Let n be the number of elements in this group. Prove that

   $$a^n = e.$$

4. Give me three distinct finite groups that are not equal to $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ or $\langle (\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \rangle$ for any n. For each example, explain why your object is a group.

5. Decode the following text!

Ovzmgiw mgfvk mgom kzm hzwkzmmiv qol mgi hopm mgom okofvlm ojj rwzaoafjfmt o lriwx qgoji gob lebbivjt aiiv pojjib fvmz idflmivpi liniwoj xfjil oazni mgi lewhopi zh ov ojfiv rjovim.

Ovb lfvpi mgfl fl vzm o vomewojjt mivoaji rzlfmfzv hzw o qgoji, mgfl rzzw fvvzpivm pwiomewi gob niwt jfmmji mfxi mz pzxi mz miwxl qfmg fml fbivmfmt ol o qgoji aihzwi fm mgiv gob mz pzxi mz miwxl qfmg vzm aifvk o qgoji ovt xzwi.

Mgfl fl o pzxrjimi wipzwb zh fml mgzekgml hwzx mgi xzxivm fm aikov fml jfhi mfjj mgi xzxivm fm ivbib fm.

Og...! Qgom'l gorrivfvk? fm mgzekgm.

Iw, idpeli xi, qgz ox F?

Gijjz?

Qgt ox F giwi? Qgom'l xt rewrzli fv jfhi?

Qgom bz F xiov at qgz ox F?

Pojx bzqv, kim o kwfr vzq ...zg! mgfl fl ov fvmiwilmfvk livlomfzv, qgom fl fm? Fm'l o lzwm zh ...toqvfvk, mfvkjfvk livlomfzv fv xt ...xt ...qijj F lerrzli F'b aimmiw lmowm hfvbfvk voxil hzw mgfvkl fh F qovm mz xoui ovt giobqot fv qgom hzw mgi loui zh qgom F lgojj pojj ov owkexivm F lgojj pojj mgi qzwjb, lz jim'l pojj fm xt lmzxopg.

Kzzb. Zzzzg, fm'l kimmfvk yefmi lmwzvk. Ovb git, qgom'l oazem mgfl qgflmjfvk wzowfvk lzevb kzfvk rolm qgom F'x lebbivjt kzfvk mz pojj xt giob? Riwgorl F pov pojj mgom ...qfvb! Fl mgom o kzzb voxi? Fm'jj bz ...riwgorl F pov hfvb o aimmiw voxi hzw fm jomiw qgiv F'ni hzevb zem qgom fm'l hzw. Fm xelm ai lzximgfvk niwt fxrzwmovm aipoeli mgiwi piwmofvjt liixl mz ai o gijj zh o jzm zh fm. Git! Qgom'l mgfl mgfvk? Mgfl ...jim'l pojj fm o mofj — tiog, mofj. Git! F pov pov wiojjt mgwolg fm oazem rwimmt kzzb pov'm F? Qzq! Qzq! Mgom hiijl kwiom! Bzilv'm liix mz opgfini niwt xepg aem F'jj rwzaoajt hfvb zem qgom fm'l hzw jomiw zv. Vzq — goni F aefjm er ovt pzgiwivm rfpmewi zh mgfvkl tim?

Vz.

Viniw xfvb, git, mgfl fl wiojjt idpfmfvk, lz xepg mz hfvb zem oazem, lz xepg mz jzzu hzwqowb mz, F'x yefmi bfsst qfmg ovmfpfromfzv ...

Zw fl fm mgi qfvb?

Mgiwi wiojjt fl o jzm zh mgom vzq flv?m fm?

Ovb qzq! Git! Qgom'l mgfl mgfvk lebbivjt pzxfvk mzqowbl xi niwt holm? Niwt niwt holm. Lz afk ovb hjom ovb wzevb, fm viibl o afk qfbi lzevbfvk voxi jfui ...zq ...zevb ...wzevb ...kwzevb! Mgom'l fm! Mgom'l o kzzb voxi ? kwzevb!

F qzvbiw fh fm qfjj ai hwfivbl qfmg xi?

Ovb mgi wilm, ohmiw o lebbiv qim mgeb, qol lfjivpi.

Pewfzeljt ivzekg, mgi zvjt mgfvk mgom qivm mgwzekg mgi xfvb zh mgi azqj zh rimevfol ol fm hijj qol “Zg vz, vzm okofv.” Xovt rizrji goni lripejomib mgom fh qi uviq idopmjt qgt mgi azqj zh rimevfol gob mgzekgm mgom qi qzejb uvzq o jzm xzwi oazem mgi vomewi zh mgi evfniwli mgov qi bz vzq.