CS 670 Spring 2015 - Solutions to HW 8

Problem 31.3-2

Given a finite cyclic group $G = \langle \alpha \rangle$ of order n, the subgroups of G can be enumerated as $\{\langle \alpha^{\frac{n}{d}} \rangle, d|n\}$. Here $d|n$ denotes that d divides n and for each such positive integer d we have a subgroup $\langle \alpha^{\frac{n}{d}} \rangle$.

- $\mathbb{Z}_9 = \langle 1 \rangle$ (written additively). Thus the subgroups are $\langle 1 \rangle, \langle 3 \rangle$ and $\langle 0 \rangle$. We now write out the subgroups: $\langle 1 \rangle = \mathbb{Z}_9$, $\langle 3 \rangle = \{3, 6, 0\}$ and $\langle 0 \rangle = \{0\}$.
- $\mathbb{Z}_{13}^* = \langle 2 \rangle$. Thus the subgroups are $\langle 2 \rangle, \langle 4 \rangle, \langle 8 \rangle, \langle 3 \rangle, \langle 12 \rangle$ and $\langle 1 \rangle$. We now write down the subgroups : $\langle 2 \rangle = \mathbb{Z}_{13}^*$, $\langle 4 \rangle = \{1, 4, 3, 12, 9, 10\}$ and so on.

Problem 31.3-5

For $n > 1$ and $a \in \mathbb{Z}_n^*$, we are given the map

$$f_a : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$$

$$x \longmapsto ax$$

Now, $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow x = y$ (The inverse a^{-1} exists as $a \in \mathbb{Z}_n^*$). Thus f_a is an injection.

Since f_a maps $\mathbb{Z}_n^*$ to itself in addition to being an injection, it is also a surjection (because $\mathbb{Z}_n^*$ is finite). Thus f_a is a permutation. The inverse map takes y to $a^{-1}y$.

Problem 31.4-1

Following the Extended-Euclid algorithm we can are able to compute that $gcd(35, 50) = 5$ and $5 = 3{\cdot}35 - 2{\cdot}50$. By Theorem 31.23 we get the first solution to the equation, $3(10/5) = 6$. Then, by Theorem 31.24, we obtain the complete set of 5 solutions, $\{6, 16, 26, 36, 46 \pmod{50}\}$.

Problem 31.5-4

By Corollary 31.29, $f(x) \equiv 0 \pmod{n}$ if and only if $f(x) \equiv 0 \pmod{n_i}$ for all i. Denote the set of roots to the equation $f(x) \equiv 0 \pmod{n_i}$ by R_i. Then the total number of k-root-tuples that satisfy all the k equations is $\prod_{i=1}^{k} |R_i|$. Each k-root-tuple uniquely corresponds to a root of $f(x) \equiv 0 \pmod{n}$.

Problem 31.7-1

The secret key d has to satisfy $ed = 1 \mod \phi(n)$. Here $\phi(n) = (p-1)(q-1) = 280$.

$$280 = 93.3 + 1 \Rightarrow 93.3 = -1 \mod 280$$

$$\Rightarrow 93^2.3^2 = 1 \mod 280 \Rightarrow (93^2.3)3 = 1 \mod 280 \Rightarrow 187.3 = 1 \mod 280$$

Thus $d = 187$ is a secret key.

The encryption of 100 is

$100^3 \mod 319 = 254$

Problem 31.7-3

Fix p, q, e. Modulo n, we have $P_A(M_1M_2) = (M_1M_2)^e = M_1^eM_2^e = P_A(M_1)P_A(M_2)$.

Claim: Let $R : \mathbb{Z}_n \to \mathbb{Z}_n$ be such that

$$|\{k \in \mathbb{Z}_n \mid R(P_A(k)) = k\}| \geq n/100.$$

If there exists an efficient procedure D_R to compute R then for every $\epsilon > 0$, there exists an efficient probabilistic algorithm T_ϵ such that for every message $M \in \mathbb{Z}_n$, the probability that $T_\epsilon(P_A(M)) = M$ is greater than $1 - \epsilon$.

Here is an informal outline of the idea behind our algorithm T. If messages could be chosen uniformly at random from $\mathbb{Z}_n$ then in expectation D_R would decode one in ten messages. However, messages are not chosen uniformly at random; they are given to us by an adversary. Therefore, we need to modify a given message M to make the modification appear as if we picked it uniformly at random from $\mathbb{Z}_n$. At the same time, decoding the modification should yield enough information to recover the original message. If we can modify M thus in ten different ways, then in expectation D_R should be able to decode at least one of these modifications. Even better, if we modify M in $10\lg(1/\epsilon)$ different ways then the probability of decoding becomes sufficiently large. We have shown that multiplication preserves information. So, let us attempt to use some sort of multiplication to arrange suitable modifications.

Case 1: $M \in \mathbb{Z}_n^*$. (Notation: $\mathbb{Z}_n^* = (\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group). We will multiply a given cipher $C = P_A(M)$ from $\mathbb{Z}_n^*$ by the encoding $P_A(X)$ of a number X chosen at random from $\mathbb{Z}_n^*$. Since P_A is a permutation on $\mathbb{Z}_n^*$, $P_A(X)$ is also distributed uniformly at random from $\mathbb{Z}_n^*$. Since $\mathbb{Z}_n^*$ is a group, the product $CP_A(X)$ is also distributed uniformly at random from $\mathbb{Z}_n^*$, and hence may be viewed as the encoding $P_A(Y)$ of an element Y picked randomly from $\mathbb{Z}_n^*$.

By the multiplicative property, this random number Y equals MX. Since we know X, if we decode $P_A(Y)$, we can easily recover M. However, since $\mathbb{Z}_n^*$ is almost of size n, the probability of decoding $P_A(Y)$ with D_R is only slightly less than .01. Hence, repeating this procedure $20\lg(1/\epsilon)$ times will certainly be sufficient to ensure a sufficiently high probability of success.

Case 2: M is divisible by p or q. Then the GCD of M and n is p or q (unless M is 0 mod$n$), and we can factor n.

Problem 31.4

a. Consider the following set of elements in $\mathbb{Z}_p^*$

$$\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$$

Claim: These are distinct elements. Assume otherwise. Say $x^2 = y^2$ in $\mathbb{Z}_p^*$ for some $x, y \in \{1, 2, \ldots, \frac{p-1}{2}\}$ and $x \neq y$. This implies $x^2 - y^2 = 0 \mod p \Rightarrow (x+y)(x-y) = 0 \mod p \Rightarrow p \mid x+y$. This is a contradiction as $x, y \in \{1, 2, \ldots, \frac{p-1}{2}\}$.

Thus the set $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ is a set of $\frac{p-1}{2}$ quadratic residues modulo p.

Let $y \in \mathbb{Z}_P^*$ be an element not in the set $\{1, 2, \ldots, \frac{p-1}{2}\}$. Then there exists a $x \in \{1, 2, \ldots, \frac{p-1}{2}\}$ such that $x + y = p$. Thus the set $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ indeed contains all the quadratic residues. Thus the number of quadratic residues is $\frac{p-1}{2}$.

b. From Fermat's little theorem, $a^{p-1} = 1 \mod p$. Hence either $a^{\frac{p-1}{2}} = 1 \mod p$ or $a^{\frac{p-1}{2}} = -1 \mod p$. If $\left(\frac{a}{p}\right) = 1$, then $\exists x \in \mathbb{Z}_p^*$ such that $x^2 = a \mod p$.

$$a^{\frac{p-1}{2}} = x^{p-1} = 1 \mod p$$

We now prove the other direction. Let $a^{\frac{p-1}{2}} = 1 \mod p$.

Let α be a primitive root $\mod p$ and $a = \alpha^i$.

$a^{\frac{p-1}{2}} = 1 \mod p \Rightarrow {\alpha^i}^{\frac{p-1}{2}} = 1 \mod p \Rightarrow p - 1/\frac{i(p-1)}{2}$

$\Rightarrow 2/i \Rightarrow \alpha^{\frac{i}{2}} \in \mathbb{Z}_p^* \Rightarrow a = {\alpha^{\frac{i}{2}}}^2 \Rightarrow \left(\frac{a}{p}\right) = 1.$

Algorithm to compute $\left(\frac{a}{p}\right)$ given a:

Compute $a^{\frac{p-1}{2}} \mod p$ by modular exponentiation. Set $\left(\frac{a}{p}\right) := 1$ if the answer is 1 and $\left(\frac{a}{p}\right) := -1$ otherwise. The running time for the exponentiation is $O(\log_2 p)$ multiplications.

c. Given $p = 4k + 3$ and $\left(\frac{a}{p}\right) = 1$.

Thus $\exists x \in \mathbb{Z}_p^*$ such that $x^2 = a \mod p$.

${a^{k+1}}^2 = a^{2(k+1)} = x^{4(k+1)} = x^{4k+4)} \mod p$.

But $p - 1 = 4k + 2 \Rightarrow x^{4k+4)} = x^{4k+2}x^2 = x^2 = a \mod p$.

Thus ${a^{k+1}}^2 = a \mod p$ and a^{k+1} is a square root of a modulo p.

We can compute a square root of a in this case by computing a^{k+1}, again the running time is dominated by the $O(\log_2 p)$ multiplications it takes to perform the exponentiation.

d. From part a, we know that half the elements of $\mathbb{Z}_p^*$ are quadratic residues and half the elements are non residues. Thus we can pick an element $a \in \mathbb{Z}_p^*$ at random and test(using part b) if its a non residue. The expected number of trials before we pick a non residue is 2. Thus the expected running time is $O(\log_2 p)$ multiplications in $\mathbb{Z}_p^*$.