CS 2800 HW #9

KIRILL CHERNYSHOV

Problem 1

(a) By definition, we know that $H_x = Ax + B$. If we have the condition $A = [a]$, then $H_x = [a]x + B$. We also know that B ranges from $[0]to[p-1]$ which means that H_x ranges from $[a]x$ to $[a]x + [p-1]$. The difference between two different values of H_x is therefore at most $[p-1]$, which means all of the possible values of B give different equivalence classes $\mod p$. Since B takes on p different values with the probability of each being $\frac{1}{p}$, then so does H_x given the condition $A = [a]$, i.e. $P(H_x = y|A = [a]) = \frac{1}{p}$. Therefore, $\sum_a P(H_x = y|A = [a]) = 1$, since there are p terms in the sum. $P(H_x = y) = \sum_a (P(H_x = y|A = [a]) \cdot P(A = [a])) = \frac{1}{p} \sum_a (P(H_x = y|A = [a]) = \frac{1}{p}$.

(b) First, I claim that, given the conditions $H_{x_1}(s) = y_1$ and $H_{x_2}(s) = y_2$ for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$, $s = ([a], [b])$ is uniquely determined.

Proof. We have $H_{x_1}([a], [b]) = y_1 = [a]x_1 + [b]$, and $H_{x_2}([a], [b]) = y_2 = [a]x_2 + [b]$. Rearrange to solve for $[b] = y_1 - [a]x_1 = y_2 - [a]x_2$. Rearrange again to get $y_1 - y_2 = [a]x_1 - [a]x_2 = [a](x_1 - x_2)$. Since p is prime, we know that any nonzero equivalence class in $\mathbb{Z}_p$ is a unit. Since both $x_1, x_2 \in \mathbb{Z}_p$ and $x_1 \neq x_2$, $x_1 - x_2 \in \mathbb{Z}_p$ and $x_1 - x_2 \neq [0]$. Therefore, $x_1 - x_2$ is a unit, that is, there exists a *unique* $[k] \in \mathbb{Z}_p$ such that $[k](x_1 - x_2) = [1]$. Multiply both sides of the equation $y_1 - y_2 = [a](x_1 - x_2)$ by $[k]$ to get $[k](y_1 - y_2) = [a](x_1 - x_2)[k] = [a][1] = [a]$. Since $[k]$ is unique, this means that $[a]$ is uniquely determined by x_1, x_2, y_1, y_2. From before we have $[b] = y_1 - [a]x_1 = y_2 - [a]x_2$, which means $[b]$ is also uniquely determined. $\square$

Two events P and Q are independent iff $P(P) \cdot P(Q) = P(P \cup Q)$. If H_{x_1} and H_{x_2} are independent, then $P = (H_{x_1} = y_1)$ and $Q = (H_{x_2} = y_2)$ are independent for all y_1, y_2. By the claim above, we know that $P(P \cup Q) = P(s = ([a], [b])) = P(A = [a] \cup B = [b])$. We are given that A and B are independent, so $P(A = [a] \cup B = [b]) = P(A = [a]) \cdot P(B = [b]) = \frac{1}{p^2}$. By the claim in part (a), we know that $P(P) = P(Q) = \frac{1}{p}$, and therefore $P(P) \cdot P(Q) = \frac{1}{p^2} = P(P \cup Q)$, and P and Q are independent for all y_1, y_2. That is, H_{x_1} and H_{x_2} are independent.

Problem 2

(a) $m = pq = 31 \cdot 23 = 713$, and $\phi(m) = (p-1)(q-1) = 30 \cdot 22 = 660$.

(b) First the public key e must be generated, with the rule that $1 \leq e \leq 660$, and $\gcd(e, 660) = 1$. Such an example is $e = 7$. The private key is the inverse of $7 \mod 660$, that is, $e \cdot d \equiv 1 \mod 660$. We can find this using the extended Euclidean algorithm, by finding $a, b \in \mathbb{Z}$ such that $7a + 660b = 1$; then, a will be the modular multiplicative inverse of 7.

We begin by dividing 660 by 7: $660 = 94 \cdot 7 + 2$. Then, $7 = 3 \cdot 2 + 1$. Rearrange the latter equation, and substitute:

$$\begin{aligned}1 = 7 - 3 \cdot 2 &= 7 + (-3)2 \\ &= 7 + (-3)(660 - 94 \cdot 7) \\ &= 283 \cdot 7 + (-3) \cdot 660\end{aligned}$$

Therefore, the private key, d, is 283, the modular multiplicative inverse of 7 mod 660.

(c) To encrypt, one must calculate $[213]^{[7]}$. Since $[213]$ is an equivalence class $\mod 713$, and $[7]$ is an equivalence class $\mod 660 = \phi(713)$, this is well defined, and equal to $[213^7] = [213^1]^1[213^2]^1[213^4]^1$, since $7 = 1 + 2 + 4 = 111_2$. To avoid having to square large numbers, we note that $[213^2]_{713} = [45369]_{713} = [450]_{713}$, and $[213^4]_{713} = [(213^2)^2]_{713} = [450^2]_{713} = [202500]_{713} = [8]_{713}$. Therefore, $[213^1][213^2][213^4] = [213][450][8] = [95850][8] = [308][8] = [2464] = [325]$.

(d) To decrypt, calculate $[47]^{[283]} = [47^{283}]$, for the same reason as above. Note that $283 = 100011011_2$, and therefore $[47^{283}] = [47^1][47^2][47^8][47^{16}][47^{256}]$. Once again, note that $[47^2] = [2209] = [70]$, $[47^4] = [(47^2)^2] = [70^2] = [4900] = [622]$, $[47^8] = [(47^4)^2] = [622^2] = [386844] = [438]$, $[47^16] = [(47^8)^2] = [438^2] = [191844] = [47]$. This means that we can skip to $[47^{256}] = [(47^{16})^{16}] = [47^{16}] = [47]$. Therefore, $[47^1][47^2][47^8][47^{16}][47^{256}] = [47][70][483][47][47] = [47][47^2][70][483] = [47][70^2][483] = [47][622][483] = [47][253] = [483]$.