Assignment #1 – Solutions

Problem 1

Use the extended Euclidean algorithm to derive $P^{-1}\ mod\ Q$ where $P = 23$ and $Q = 89$.

i	x_i	y_i	a_i	b_i	q_i
1	1	0	89	23	
2	0	1	23	20	3
3	1	-3	20	3	1
4	-1	4	3	2	6
5	7	-27	2	1	1
6	-8	31	1	0	2
7	23	-89			

$P^{-1}\ mod\ Q$ = 31.

Problem 2

- $z_1 = m^3 \bmod N_1$, $z_2 = m^3 \bmod N_2$, and $z_3 = m^3 \bmod N_3$.

Assume N_1, N_2, and N_3 have no common factors.
(If not, take a GCD, factor one of the N_i, and decrypt m.)

Use the Chinese Remainder Algorithm to find z such that
$z \bmod N_1 = z_1$ and $z \bmod N_2 = z_2$.
Use CRA again to find Z such that $Z \bmod N_1 N_2 = z$
and $Z \bmod N_3 = z_3$.

This $Z \equiv m^3 (\bmod N_1 N_2 N_3)$. But $m^3 < N_1 N_2 N_3$, so $m = \sqrt[3]{Z}$.

Problem 3

Get public modulus N and exponent e from device.

Take message m, compute encryption $z = m^e \bmod N$, give z to device and receive back incorrect decryption m'.

By assumption, $m \equiv m' \pmod{P}$, but $m \not\equiv m' \pmod{Q}$.
Compute GCD($m - m'$,N).

Since $m - m' \equiv 0 \pmod{P}$, $m - m'$ is a multiple of P.
Since $m - m' \not\equiv 0 \pmod{Q}$, $m - m'$ is not a multiple of Q.

Hence GCD($m - m'$,N) $= P$. $Q = N/P$.

Problem 4

Bob sends to Alice:

$$[E_A(\text{Bob's order}), E_A(\text{Bob's credit card})]$$

You to Alice:

$$[E_A(\text{Your order}), E_A(\text{Bob's credit card})]$$

Problem 5

- $A = Y^a \bmod N$, $B = Y^b \bmod N$, and $C = Y^c \bmod N$.

Trick Question!!!

$Y^{abc} \bmod N$ would be a lovely key – if they could compute it; but they can't without revealing a, b, or c.

One answer: Alice picks a random key K, and computes joint keys $Y^{ab} \bmod N$ and $Y^{ac} \bmod N$ to send K to each of Bob and Carol. Bob and Carol can use their joint key to confirm that they received the same K from Alice.