Prob 45

$$v = [g^{u_1} y^{u_2} \bmod p] \bmod q \stackrel{?}{=} r = [y^z \bmod p] \bmod q$$

$$[(g^{u_1} \bmod p)(y^{u_2} \bmod p)] \bmod p \bmod q \qquad g = p+1$$

$$\{[\underbrace{(p+1) \bmod p}_{1}]^{u_1} \bmod p \ (y^{u_2} \bmod p)\} \bmod p \bmod q$$

$$[y^{u_2} \bmod p] \bmod q \stackrel{?}{=} [y^z \bmod p] \bmod q \qquad u_2 = r(s^{-1} \bmod q) \bmod q$$
$$s = rz^{-1} \bmod q$$

$$\Longrightarrow u_2 \stackrel{?}{=} z$$

$$r(s^{-1} \bmod q) \bmod q$$

$$r([rz^{-1} \bmod q]^{-1} \bmod q) \bmod q$$

$$r((rz^{-1})^{-1} \bmod q) \bmod q$$

$$r(r^{-1} z \bmod q) \bmod q \qquad r = r \bmod q$$

$$\cancel{r r^{-1}} z \bmod q \stackrel{?}{=} z$$

- This is true when N = hash digest size which is so for $N = 120$ and SHA-1