Daren Liu: Blue   Ryan Summers: Red

EIG 5) P=nextprime(10^24)

$g = 5$

a= \r b1FFkey.txt

$H = 2067\ldots$

K= \r b1MOkey.txt

$r = \text{Mod}(g\hat{}K, P) = 5391\ldots$

$x = K^{-1}(H+ar) \text{ Mod } p-1 = 4969\ldots$

ii) Partner's $(r, x, H) = (8438\ldots, 6766\ \ldots, 2067)$

$g^{H+ar} \bmod p = r^{x} \bmod p$

MAC 2) 1011 0110 1110 0110

$= 46822$

$n = 2314\ldots$

$e = 7269\ldots$

$d = 1071\ldots$

$M = H^{d} \bmod n = 2262\ldots$

$H = M^{e} \bmod n = 46822$

MAC 3)

$H = 46822$

$P = \mathrm{nextprime}(10^\wedge 24)$

$g = 5$

$k = 7178\ldots$

$a = 6000\ldots$

$r = g^k \bmod p = 5391\ldots$

$x = k^{-1}(H + ar)(\bmod p - 1) = 4174\ldots$

Verify with $g^{H+ar} \bmod p = r^x \bmod p$