My color: Blue Partner's color: Red

RSA 4.5) Person 1: $r_1 r_2$ $e = 17$

Person 2: $r_1 r_2$

Person 3: $r_3 r_4$

Person 4: $r_3 r_5$

i) Person 2 since he shares the same n, p, q values as person 1.

ii) Person 4. If person person 3 and person 4 share r_3, then Person 4 can solve for r_4 since n and e are published.

DH-1) a) $g = 2$ $a_A = 13$

$g^{a_A} \pmod{677} = 68$

b) $J^{a_B} = 287$ $g = 2$

$g^{(a_A)(a_B)} = 287^{a_A} \pmod{677} = 197$

c) $197/26 = 7$ $197 \% 26 = 15$

$(a, b) = 7, 15$

PT = YO $C \equiv 7P + 15 \pmod{26}$

$Y = 24$ $(7(24)+15) \pmod{26} = 1$

$O = 14$ $(7(14)+15) \pmod{26} = 9$

CT = BJ

DH-2) My public key = 2580...

Partner public key = 6353...

Shared key = 1361...

Reduced shared key = 38671

DH-3) ed = 4835... Shared key = 1115...

Key = 9293

PT = Blue man group

DH-4) Private key = 8675309

$q = 2^{125}$

Mod(Public key, q) ^ private key =

$x^{23} + x^{22} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^5 + x^3 + x + 1$

$q_{24} - q_9 = 0110\,1001\,1111\,1001$

PT = Whit and Marty