Homework 3 Ex 10 (c) and (d) 08.11.'11

(c)

1: $A \xrightarrow{n} B$ // $n = p^2$

2: $B \xrightarrow{y} A$ // $y \equiv x^2 \pmod n$

$\equiv x^2 \pmod{p^2}$

3: $A \xrightarrow{\pm x} B$

// there are only two solutions, so that A is always right (cf. (b))

// B cannot factor n: $\gcd(x - (\pm x), n)$

1) $\gcd(0, n) = n$

2) $\gcd(2x, n) = \gcd(2xp^2) = p^2 = n$

(d) i) If Bob asks for the secret key as confirmation, the squeeze is revealed and A will be accused of cheating.

ii) B can factor n by $p = \sqrt{n}$ (in the reals) and wins the game. However, he can be an honest player and proceeds as in i) without loosing the game.