Exam Corrections

1

c

Why does this algorithm require a trusted third party?

✓ **Answer**

Unless you've exchanged public keys on an already established and secure channel, you have no idea if the public keys exchanges were tampered with before transmission, therefore a trusted third party is normally in charge of generating the public parameters to ensure both sides have a fair communication. In other signing methods, this third party also has their own public key, which they may sign provided parameters with in order to further improve trust on an unsecure channel.

4

a

What is a Blum integer?

✓ **Answer**

A Blum integer is a semiprime which both parts are congruent to $3 \pmod 4$, and thus the jacobi of $\left(\frac{-1}{pq}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) = (-1)(-1) = 1$.

b

If p is a prime congruent to $3 \pmod 4$ and the equation $x^2 \equiv a \pmod p$ has solutions, give a formula for the solutions.

✓ **Answer**

$p = 4k + 3 \implies \frac{p+1}{4} = k + 1 \in \mathbb{Z}$

$(a^{(p+1)/4})^2 = a^{(p+1)/2} = aa^{(p-1)/2} = a$

$x = \pm a^{(p+1)/4}$

c

If the equation above does not have any solutions, what does the formula give?

✓ **Answer**

$a^{(p-1)/2} = -1$ instead, so it would give $-a$