Explain what is a Zero Knowledge Proof.

Zero knowledge proof is a **protocol**, in cryptography, that allows one party to convince another party that he/she knows a secret (e.g., his/her private key) without revealing to the other party the secret. One example is as follow:

$y = g^{x} mod\, p$

$H(g^{a}y^{b}) = a$

1) $random\, z$
2) $a = H(g^{z})$
3) $a + xb = z\, mod\, p$
    $xb = z - a\, mod\, p$
    $b = (z - a)x^{-1}\, mod\, p$

$Output$: $(a, b)\ such\ that\ H(g^{a}y^{b}) = a$

Proof:
$H(g^{a}y^{b}) = H(g^{a}(g^{x})^{b}) = H(g^{a+bx})$

The scenario explanation:

(i) Alice knows x, her private key.
(ii) Alice computes $y = g^{x} mod\, p$ and passes y to Bob.
(iii) To prove to Bob that Alice indeed knows the value of x without revealing the value of x to Bob, Alice does the following:
    i. Chooses a random value z
    ii. Computes two values a and b:
        - $a = H(g^{z})$, and
        - $a + xb = z\, mod\, p$
          $xb = z - a\, mod\, p$
          $b = (z - a)x^{-1}\, mod\, p$

    and output $(a, b)\ such\ that\ H(g^{a}y^{b}) = a$

(iv) Alice sends $H(g^{a}y^{b}) = a$ to Bob. Note: The value of a is computed involving the value of x.
(v) Bob, in order to convince that Alice knows x, Bob, will randomly chooses two values for a and b and asks Alice to compute $H(g^{a}y^{b})$.

(vi) Bob will verify that $H(g^a y^b) = a$, and after a few verification (with different values of a and b), Bob will be convince that Alice indeed knows the value of x, because both the values of a and y in $H(g^a y^b)$ are computed involving the value of x.