Question 1 Solution:

Prove:

Assume toward contradiction that G is not an OWF, so there exists an adversary A that inverts G with non-negligible probabiity: given $G(x) = y$, A can find x. We can then construct adversary B using A that distinguishes the output of G from a random string.

B works:

1) Takes a string y as input, where y mght be the output of G or a random string.

2) B runs A on y to find an x such that $G(x) = y$

3) If A successes in finding such an x, then B indicates that y is the output of G; otherwise, B indicates that y is a random string.

Analysis:

If y is the output of G, then it must have a preimage x that is half the length of y for which A successfully find with non-negligible probability.

If y is a random string, then the proability of A finding its preimage x is merely at most (assuming G is a permutation) $\frac{2^{n/2}}{2^n} = \frac{1}{2^{n/2}}$ which is negligible. This is the probability that y falls in the range of G.

Therefore the probability that B distinguishes the output of G from a random string is non-negligible minus negligible probability, which is negligible. This shall not be the case for G the generator, so G must not be an OWF.

Question 2 Solution:

a): Alice outputs k

Bob outputs $k' =$

$$w \oplus t$$

$=$

$$u \oplus r \oplus t$$

$=$

$$s \oplus t \oplus r \oplus t$$

$=$

$$k \oplus r \oplus t \oplus r \oplus t$$

$= k$

b): This protocol is secure.

To prove the secutity of the key exchange protocol, we need to show that given the transcript which includes s= k XOR r and $u = s$ XOR t $w = u$ XOR r, no PPT adversary can computer k with non-negligible probability.

However, since r and t are random, the adversary sees s, u and w all as random strings. In other words, if the adversary could find k then it means it can determine random strings which is inherently impossible.