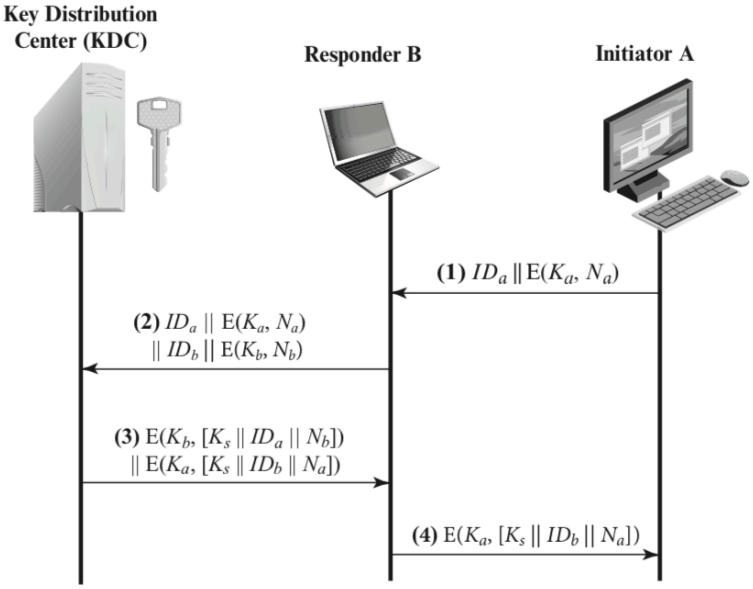
4. An alternative key distribution method suggested by a network vendor is illustrated in the figure below.

illustrated in the figure below.



1. (a) Describe the scheme in steps.
2. (b) How do A and B know that the key is freshly generated?
3. (c) How could A and B know that the key is not available to other users in the system?
4. (d) Does this scheme ensure the authenticity of both A and B? Justify your answer.
5. Consider the following hash function based on RSA. The key < n, e > is known to the public. A message M is represented by blocks of predefined fixed size M_1, M_2, M_3, ..., M_m such that $M_i < n$. The hash is constructed by XOR the results of encrypting all blocks. For example, the hash value of a message consisting of three blocks is calculated by

$H(M) = H(M_1,M_2,M_3) = (M_1^e \bmod n) \oplus (M_2^e \bmod n) \oplus (M_3^e \bmod n)$

Does this hash function satisfy each of the following requirements? Justify your an-swers (with examples if necessary).

(a) Variable input size (b) Fixed output size

(c) Efficiency (easy to calculate) (d) Preimage resistant

(e) Second preimage resistant (f) Collision resistant