Crypto 1

In an electronic auction, bidder Bob casts his bid B encrypting it by means of the auctioneer Alice's public key pubKA (2048 bit). Let us assume that a bid is 32-bit unsigned and is uniformly distributed. Argue whether the protocols in the figure are practical and secure w.r.t. to a passive adversary who attempts to guess the bid B. A protocol is secure if the guessing attack requires at least 2 to 80 steps.

In the protocols, H(·) is a secure hash function whose output size is h-bit, R is an r-bit random number, and K is a k-bit random symmetric cryptographic key. R and K are generated dynamically at bidding time. For each protocol, specify the values of h, r and k for which the protocol is secure.

Argue the case the bid B is not uniformly distributed but falls in the interval [B1, B2], with B1, B2 unsigned and B1 < B2.

1. $B \rightarrow A$: Bob, $\{Bob, B\}_{pubKA}$
2. $B \rightarrow A$: Bob, $\{Bob, B, H(B))\}_{pubKA}$
3. $B \rightarrow A$: Bob, $\{Bob, H(B)\}_{pubkA}$
4. $B \rightarrow A$: Bob, R, $\{Bob, R, B\}_{pubKA}$
5. $B \rightarrow A$: Bob, $\{Bob, R, B\}_{pubKA}$
6. $B \rightarrow A$: Bob, $\{Bob, K\}_{pubKA}$, $\{Bob, B\}_K$

SOLUTION:

1. **Insecure**. The ciphertext is an oracle. $O(2^{32})$.
2. **Insecure**. Same reasoning as case 1. Using a different hash function has no effect.
3. **Insecure**. In addition, this scheme is useless because the auctioner would have to guess the the bid. CT is still an oracle. $O(2^{32})$. Changing hash function H(·) has no effect.
4. **Insecure**. Same reasoning as 1 and 2 because R is sent in the clear and thus the guessing is still only on B.
5. **Secure**. R must be at least on $r \geq 80 - 32 = 48$ bit.
6. **Secure**. The adversary has to guess the symmetric key K. Thus, in order to have a security level of 80 bit, the encryption key K must be at least 80 bits.

In case B is in [B1, B2], assuming B2-B1 on p bit, $p \leq 32$, then in protocol 5, R must be $r \geq (80 - p)$ bits.