Crypto 1

In an electronic auction, bidder Bob casts his bid B encrypting it by means of the auctioneer Alice's public key pubKA. 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.

Select parameters h, r and k so that secure protocols have 128-bit security level.

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,$\{Bob, K\}_{pubKA}$, $\{Bob, B\}_{K}$