Quiz - Five most important Qs?

Topic: Security
- Basics
- In WSN.

WSN

Goal: Secure & efficient key distribution mechanism allowing simple key establishment for large-scale WSN.

Approaches:
1. Network wide shared key
   - Simple
   - Difficult to change
   - Entire network is compromised even if only a single node is compromised.
2. Pair-wise key using PKI (Diff-Hellman)
   - too expensive - key-setup latency, overhead
3. Pre-configured pair-wise shared key
   - not scalable - each node has to store (N-1) keys.
4. Bootstrapping keys using a trusted base-station - each node has a pre-configured shared key with the BS.

Diagram:

```
 AO
  v
 B0
 KA-B
 KA-A1(KA-B, BS)
 KA-A(KA-B, A)
```

4. KA-B
   - time (increased latency - messages)
     => more b/w & energy
   - BS is single point of failure
     + BS can be made tamper-resistant - amortizing the cost of physical security
5. Random Key Pre-distribution

1. for each node

2. Randomly

3. Deploy the nodes

Large Pool of Keys

Pre-Deployment-Time

Two nodes can communicate securely if they have a non-null intersection of their pre-deployed key set.