1. Significant items in a certificate are:
- the protocol used (TLS/SSL),
- the issuer CA,
- the cryptographic algorithm employed by the CA to create its own digital signature,
- the name of the entity for which the certificate is issued,
- the keys of the certified entity,
- the validity period (expiration date).

2. Since the connection is wireless and therefore unreliable, errors and losses would probably occur too frequently. Since we will have no error correction or retransmissions, we need a mode which guarantees the smallest possible error propagation from previous transmissions or losses, so that the rest of the conversation will not be prevented. Output Feedback Mode (OFB) fits these requirements where the IV has to be sent in each packet. Other acceptable solutions would be CFB and CBC. CTR mode will work, too, if the counter field is separated into packet#/block# fields and the packet# field is in each packet.

Stream cipher like RC4 is not suitable.

3. The important things given in the setting of the problem are the following: wired-in key, multiple time values will be encrypted.

In a stream cipher we cannot use the same key for multiple encryptions. In order to use a stream cipher we will need a sequence of keys. This creates difficulty for key synchronization between device and server

On the other hand we can use a block cipher in some mode of encryption to encrypt multiple time stamps with the same key. It is important though that we do not use the same IV with the same key. So we have to choose different IVs but this will not be problem since the IV does not have to be kept secret.