Solution set 10: Quantum cryptography

1) All of the communication between Alice and Bob can be made over public channels (also authentication can be done over public channels). Alice's original bit string must be sent over a quantum channel, using one of two basis, randomly chosen for each bit (this channel need not be private: if Eve is eavesdropping, Alice and Bob will notice). Comparing their basis and checking whether Eve was listening in can all be done over classical channels.

2) Alice and Bob can each measure their respective qubits in one of two basis (e.g. the computational basis, $\{|0\rangle, |1\rangle\}$ and the basis $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. The protocol then works analogously to the BB84 protocol, only they will get opposite outcomes with certainty whenever they happen to measure in the same basis. When they happen to measure in different basis, their measurement outcomes will be uncorrelated. This scheme was invented by Arthur Ekert in 1991, and is known as Ekert 91.