Diffie-Hellman Key Exchange

- First published public-key algorithm
- A number of commercial products employ this key exchange technique
- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- The algorithm itself is limited to the exchange of secret values
- Its effectiveness depends on the difficulty of computing discrete logarithms

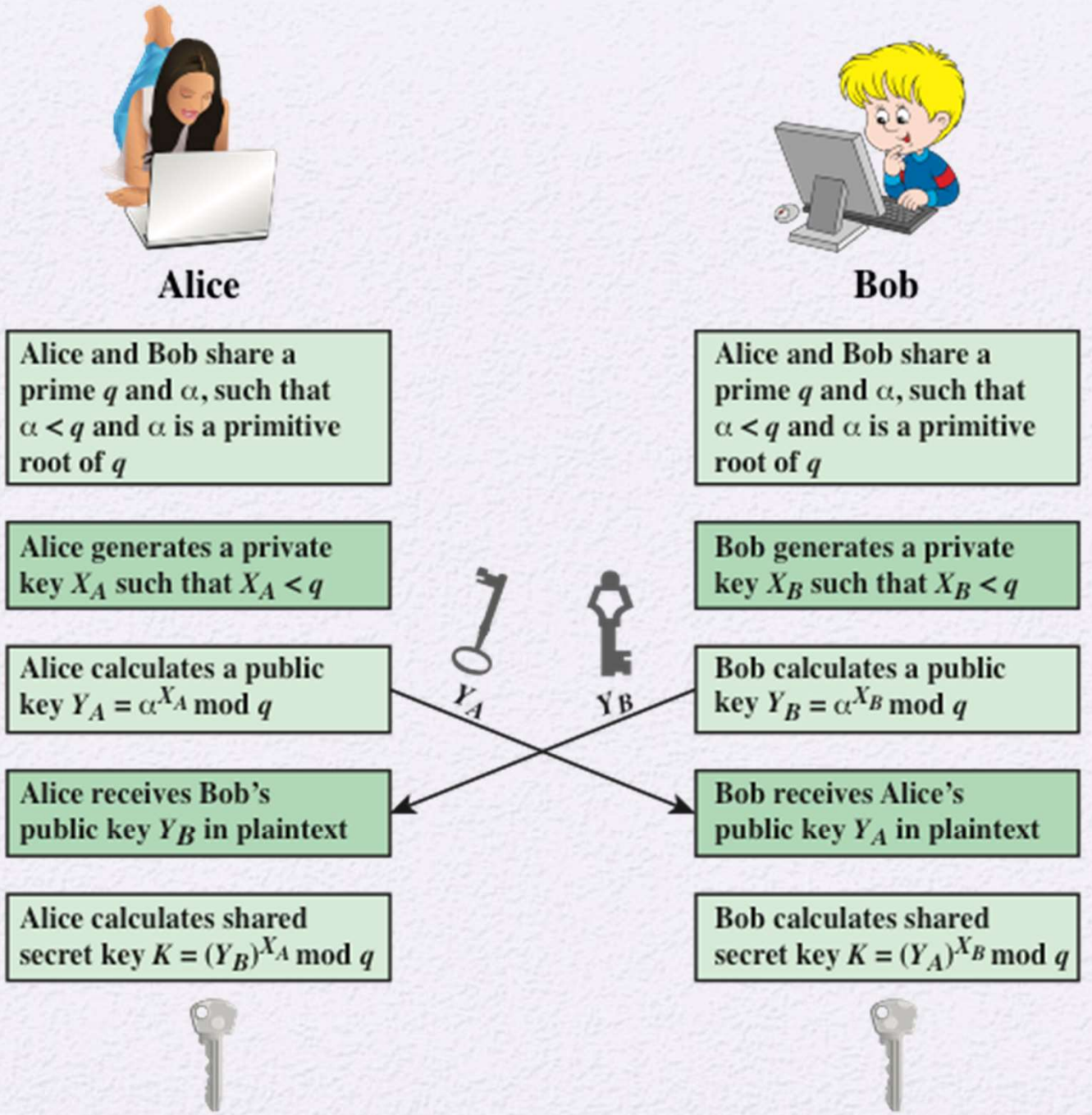

Figure 10.1 Diffie-Hellman Key Exchange

Key Exchange Protocols

- Users could create random private/public Diffie-Hellman keys each time they communicate
- Users could create a known private/public Diffie-Hellman key and publish in a directory, then consulted and used to securely communicate with them
- Vulnerable to Man-in-the-Middle-Attack
- Authentication of the keys is needed

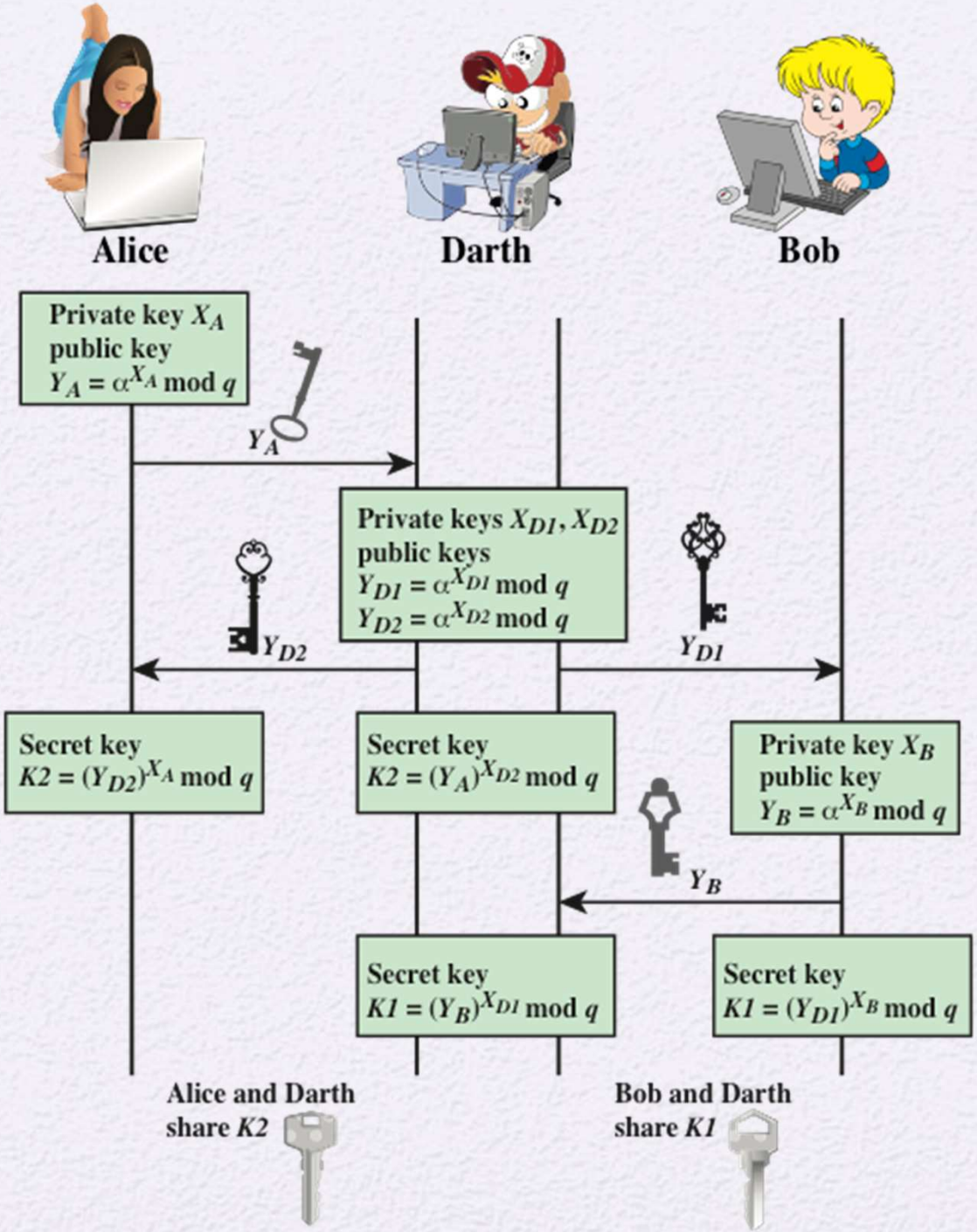

Figure 10.2 Man-in-the-Middle Attack