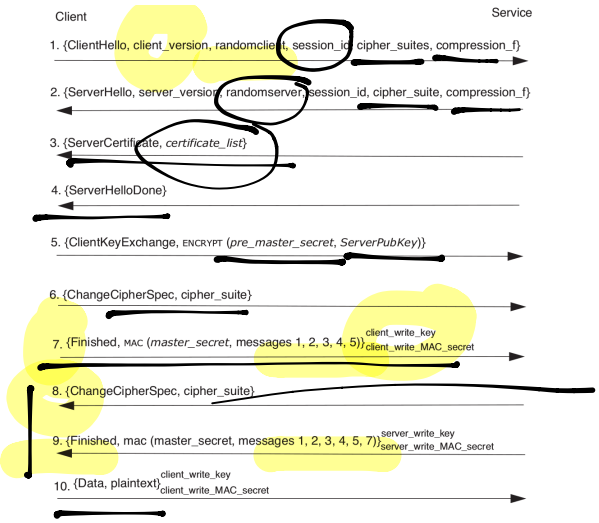
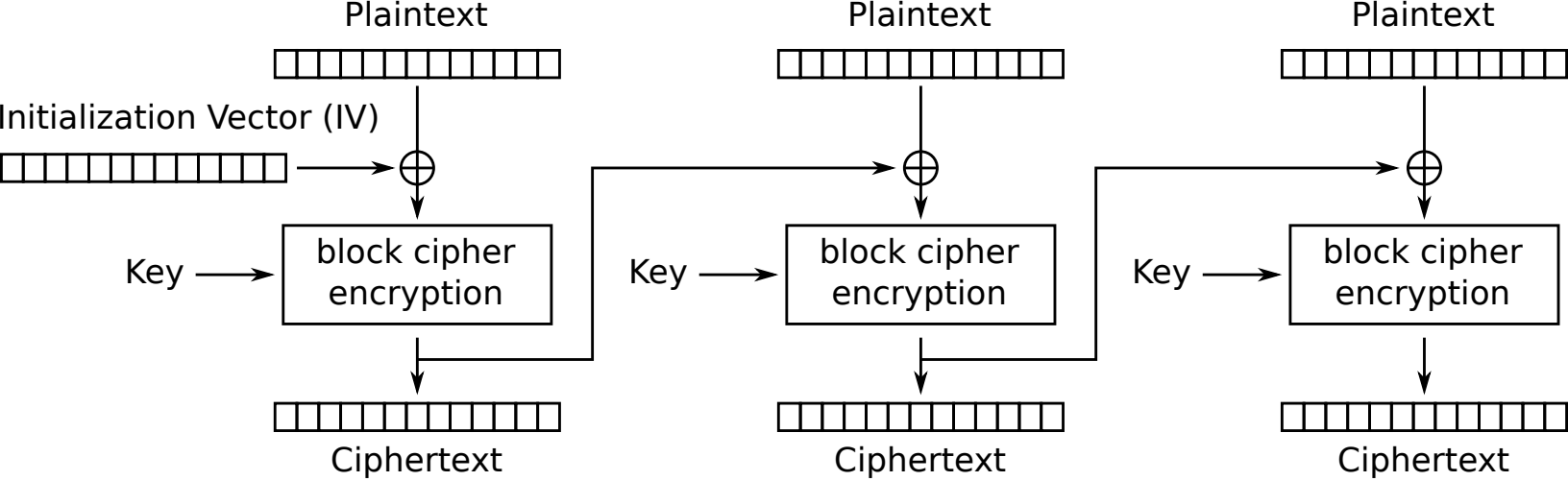

Client
Service
1. {ClientHello, client_version, randomclient, session_id, cipher_suites, compression_f}
2. {ServerHello, server_version, randomserver, session_id, cipher_suite, compression_f}
3. {ServerCertificate, certificate_list}
4. {ServerHelloDone}
5. {ClientKeyExchange, ENCRYPT (pre_master_secret, ServerPubKey)}
6. {ChangeCipherSpec, cipher_suite}
7. {Finished, MAC (master_secret, messages 1, 2, 3, 4, 5)}client_write_key client_write_MAC_secret
8. {ChangeCipherSpec, cipher_suite}
9. {Finished, mac (master_secret, messages 1, 2, 3, 4, 5, 7)}server_write_key server_write_MAC_secret
10. {Data, plaintext}client_write_key client_write_MAC_secret



Cipher Block Chaining (CBC) mode encryption