现代密码学作业——第九讲

（1）向KDC发送标识符IDA,IDB说明A发起协议,要与B通信。

（2）KDC向A发送用它的私钥sk-KDC加密的pkB,IDB。

（3）A用KDC的公钥解密消息2,得到B的公钥pk,向B发送临时值NA和IDA。

（4）B向KDC发送发送标识符IDA,IDB说明B发起协议,要与A通信。

（5）KDC向b发送用它的私钥sk-KDC加密的pkB,IDA。

（6）B用KDC的公钥解密消息5,得到A的公钥pkA,向A发送加密后的临时值IDB、NA和NB。

（7）A向B表明收到了NB。

（8）共享的密钥通过N和NB构造,例如KAB=h(NA,NB)。