



注:key是DH协商的会话密钥