第三次作业

计15 宋驰 2021010797

实现了基于 sha256 的 PRF-HMAC-SHA-256、AES-GCM-128、基于 HMAC-SHA256 的 HKDF，最后补全了 doubleratchet.cpp 中的 on_receiving_message 函数、messenger.cpp 中的 receive_message 函数。

简答题

1.What is Forward security? How does Double ratchet achieve Forward security?

A:

前向安全性确保了即使长期密钥被泄露，之前的会话密钥仍然是安全的，生成器的过去输入对于攻击者来说是随机的。即使攻击者在之后获得了内部状态，他们也无法推导出之前的密钥。

Double Ratchet中的KDF链提供了前向安全性，因为它基于HMAC。攻击者无法重现之前KDF步骤的输入，因此输出看起来是随机的。

2.What is Break-in Recovery? How does Double ratchet achieve Break-in Recovery?

A:

突破恢复指在一次妥协之后，密码协议能够恢复安全性的能力。即使攻击者获得了当前的内部状态，只要生成器被刷新并包含足够的熵，未来的输出看起来也是随机的。

Double Ratchet通过以下方式实现突破恢复：

- 使用Diffie-Hellman密钥交换作为KDF链的输入。DH输出本质上是随机的，因此当攻击者只知道当前KDF密钥时，他们无法生成相同的KDF输出。
- 每次新的DH密钥交换都会引入新的熵，确保了生成器能够恢复安全性，攻击者无法推导出未来的密钥。

3.What if they never update their DH keys at all? Please explain the security consequences of this change with regards to Forward Secrecy and Break-in Recovery.

A:

前向安全性：不更新DH密钥会降低前向安全性。虽然KDF链基于哈希函数，攻击者仍然难以计算出之前的输出密钥，因此在一定程度上仍提供前向安全性。但如果攻击者获得了当前密钥，他们可以推导出所有过去的密钥，前向安全性不再有效。

突破恢复：不更新DH密钥将导致生成器没有新的熵来源，从而不满足突破恢复的条件。一旦密钥被破坏，攻击者可以继续解密所有未来的消息。定期更新DH密钥确保生成器有足够的熵来恢复安全性，因此不更新DH密钥会使突破恢复失效。

4.Consider the following conversation between Alice and Bob, protected via the Double Ratchet Algorithm according to the spec:
A: Hey Bob , can you send me the locker combo?
A: I need to get my laptop
B: Sure , it's 1 2 3 4!
A: Great , thanks! I used it and deleted the previous message .
B: Did it work?
What is the length of the longest sending chain used by Alice? By Bob? Please explain.

A:

消息发送的顺序是AABAB。当接收到新的DH公钥时，接收者将执行DH ratchet并重置发送/接收链。

Alice首先在她的第一个发送链中发送了两条消息，然后Bob在他的第一个发送链中发送了一条消息，重置了Alice的链，Alice然后在她的第二个发送链中发送了一条消息，重置了Bob的链。

所以Alice的最长发送链是2，而Bob的最长发送链是1。

5.Unfortunately, in the situation above, Mallory has been monitoring their communications and finally managed to compromise Alice's phone and steal all her keys just before she sent her third message. Mallory will be unable to determine the locker combination. State and describe the relevant security property and justify why double ratchet provides this property.

A:

相关的安全属性是前向安全性，前向安全性确保了即使攻击者破坏当前的密钥，也无法解密之前的消息。Mallory在Alice发送第三条消息之前破坏了他的手机，可以访问Alice用于加密第三条消息及之后消息的密钥，也只能获得新发送链的密钥，但无法访问Alice和Bob用于加密之前消息的密钥，无法解密之前交换的消息，无法重新生成Bob最后一条消息的接收密钥，因此无法确定储物柜的组合。