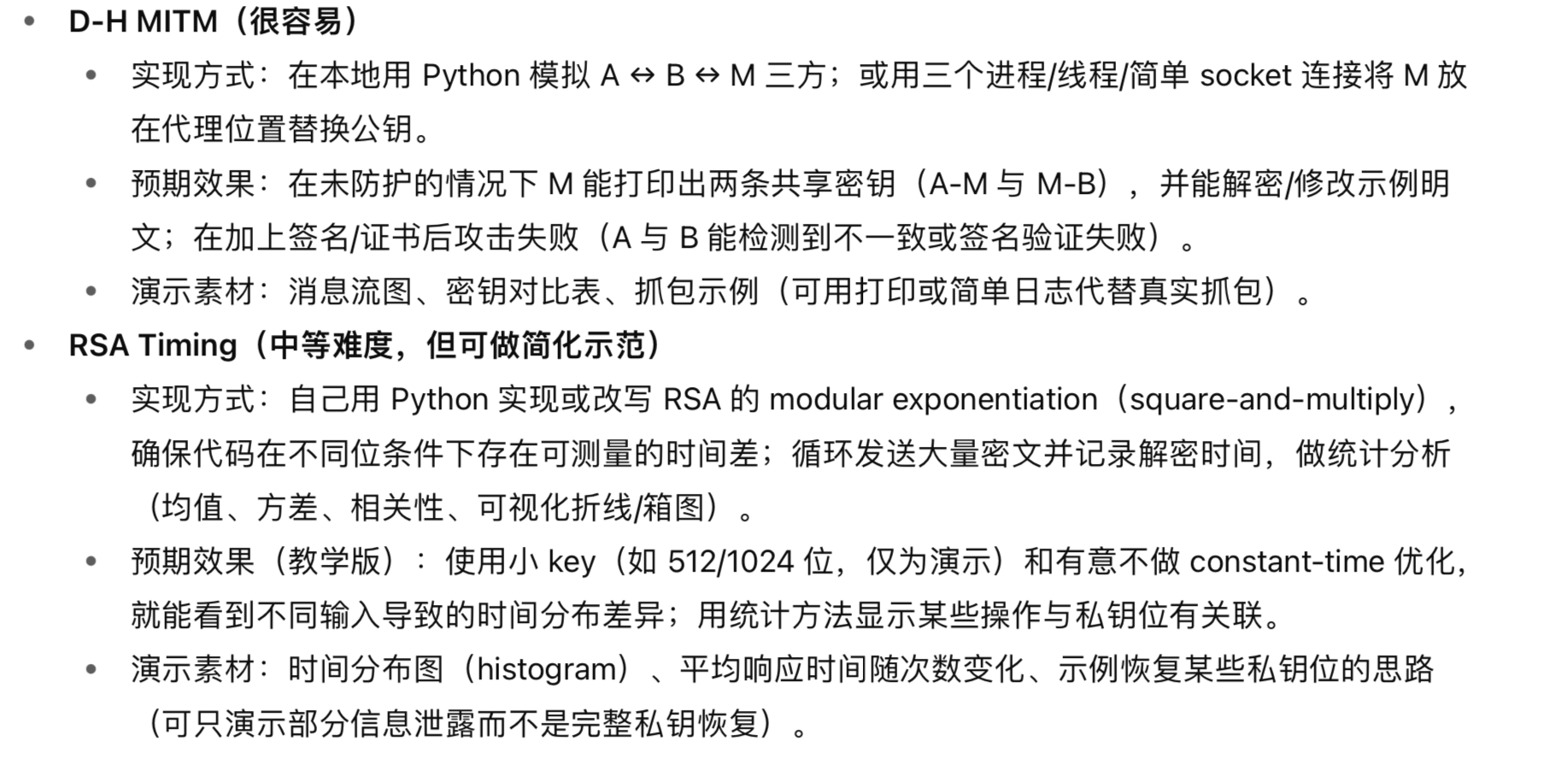
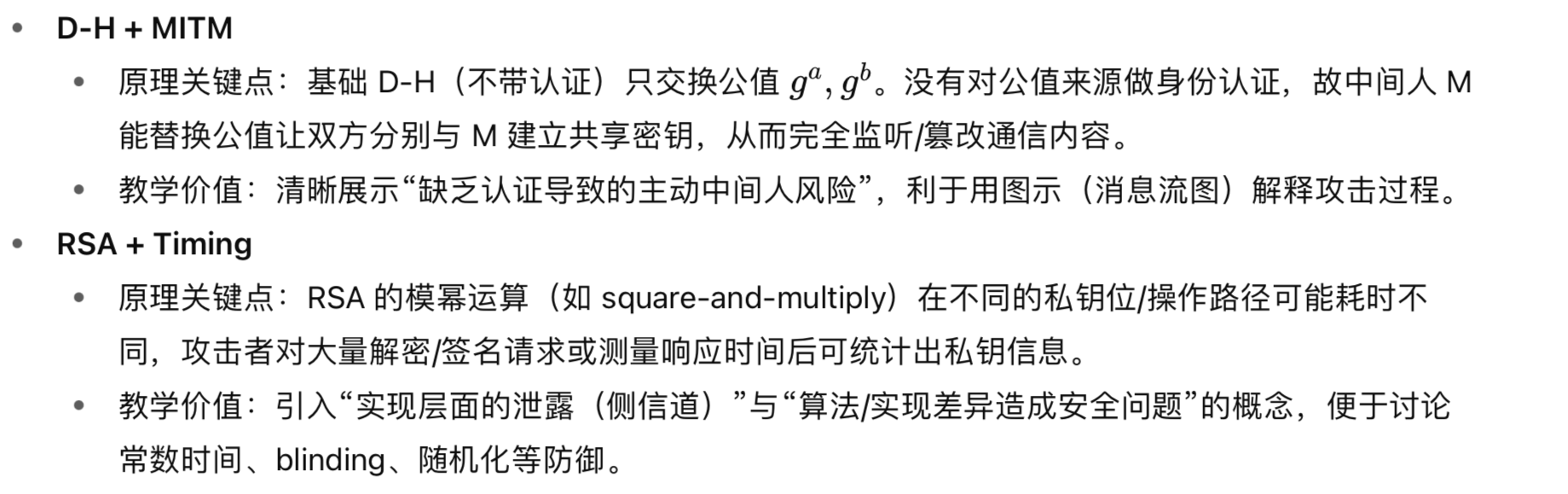
**一．两种方法的简介（没有intext引用，可以结合轩找的进行修改）**

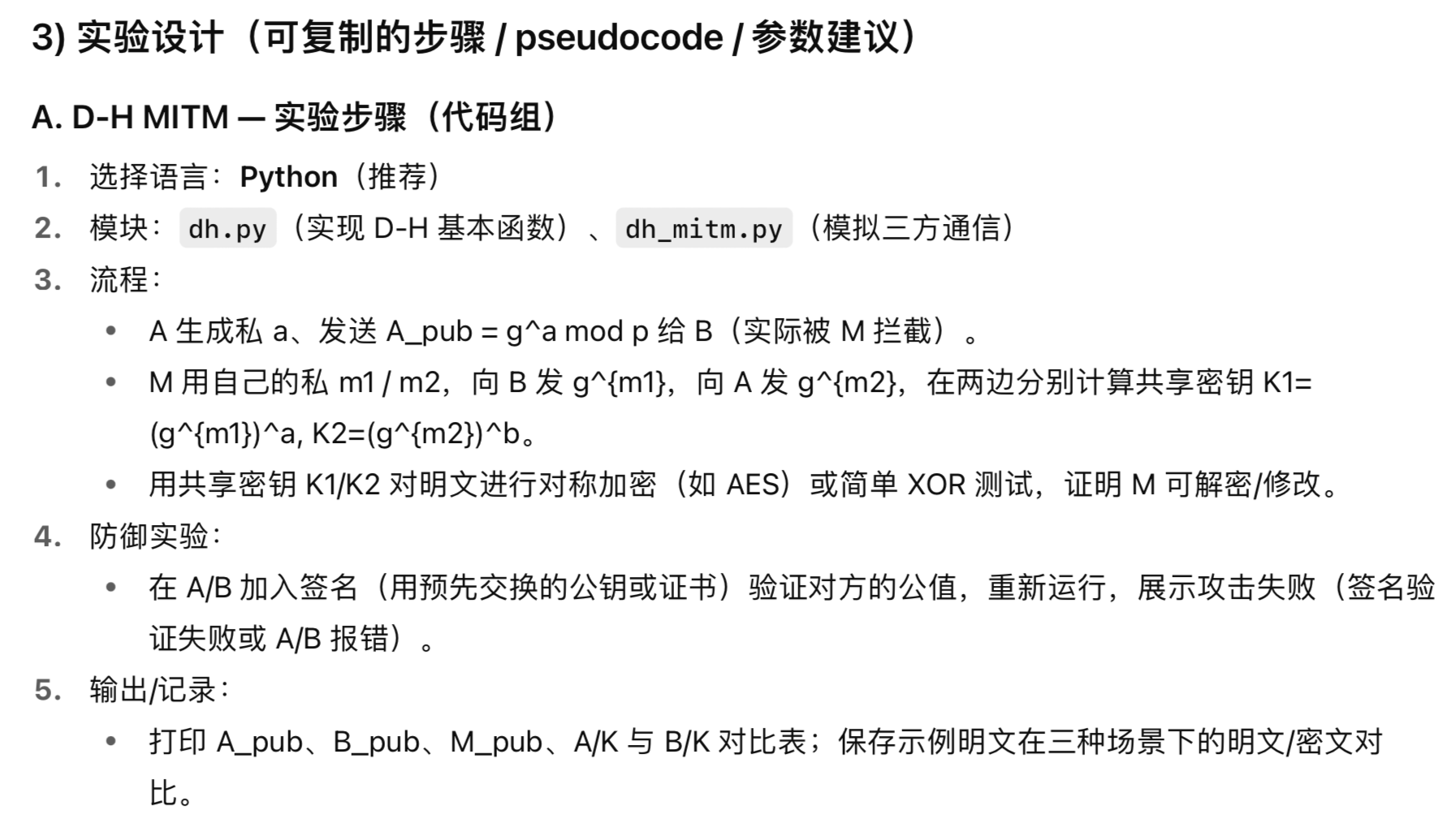
**Diffie–Hellman (D-H):**  
Diffie–Hellman (D-H), first introduced by Diffie and Hellman in 1976, is a foundational public-key agreement protocol that allows two parties to establish a shared secret over an insecure channel. The protocol relies on the difficulty of the discrete logarithm problem in a finite cyclic group: each party selects a private exponent and exchanges the corresponding public values; the shared secret is computed by exponentiation of the received public value with the local private exponent. D-H underpins many key exchange mechanisms but, in its basic form, lacks entity authentication and therefore is vulnerable to active network attacks if additional protections are not applied.

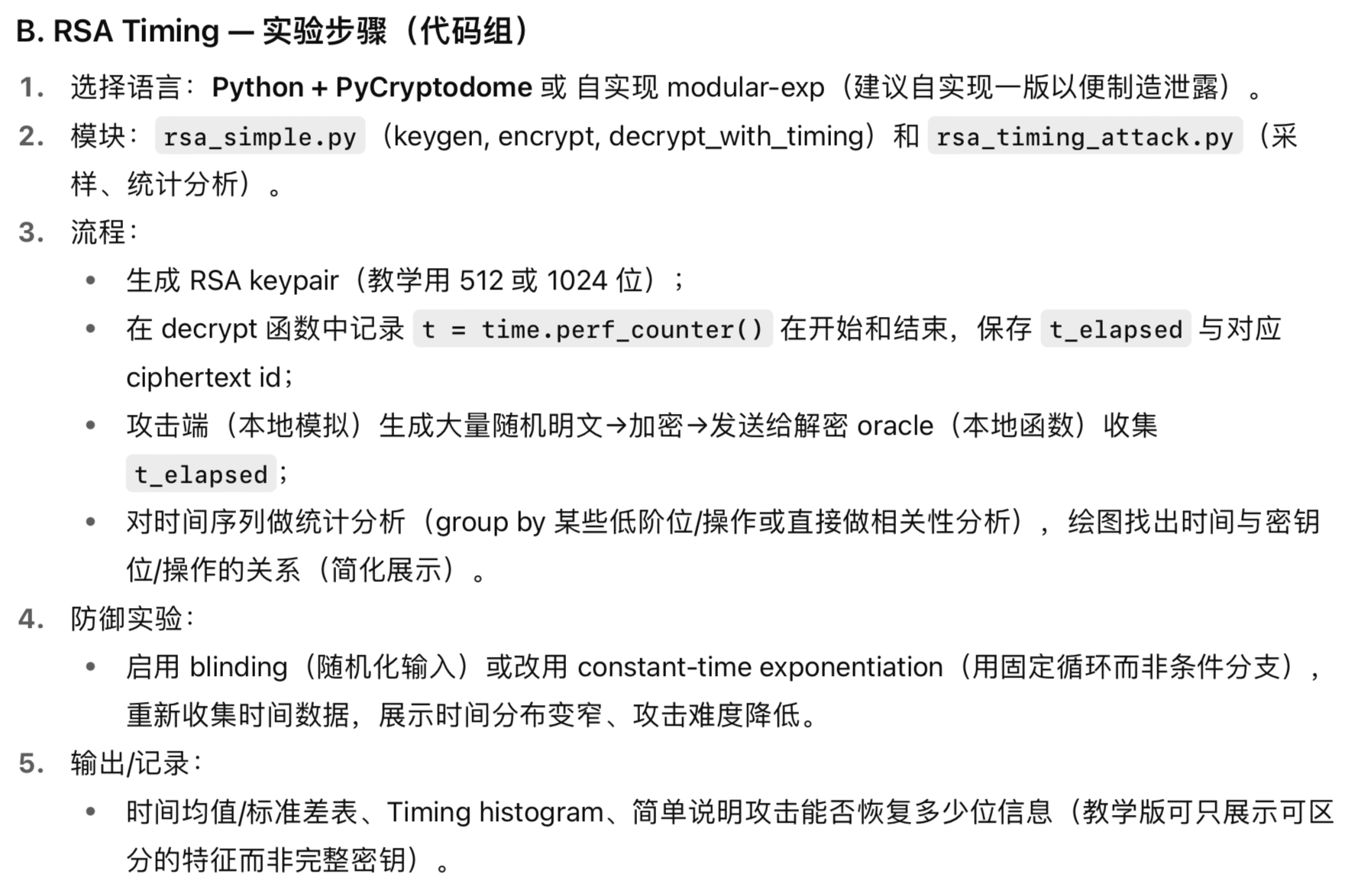
**RSA (as key transport):**  
RSA, introduced by Rivest, Shamir and Adleman, is widely used for both encryption and digital signatures. In key exchange contexts, RSA can be used to encrypt a symmetric key that is then used for session communication. RSA security relies on the pragmatic difficulty of factoring large integers; however, practical implementations can be vulnerable to attacks beyond pure mathematical factoring (e.g., side-channel attacks) if the implementation leaks information such as timing, power consumption, or error responses.

1. **觉得好写好实现的技术**

对于D-H选择MITM 对于RSA选择TIMING







1. **可能能用上的参考文献**
2. Paul C. Kocher – “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”（Springer）

主要内容：时间侧信道如何用于对 RSA 和 D-H（及 DSS）实施攻击，并且提出几种防御思路，写RSA timing attack的理论基础时可用。

1. “Authenticated Key Exchange Provably Secure against the Man-in-the-Middle”（Springer）

主要内容：讨论一种经过认证的密钥交换协议，从理论上保证它不容易受到 MITM 攻击。写D-H的防御部分可用。

1. “Preventing Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Protocol”（research gate）

主要内容：综述了对 D-H 的 MITM 攻击与已有防御方法，并提出一种新方法增强随机性 /完整性验证的方案。可用于写防御部分的参考。

1. Detector: An approach for detecting, isolating, and preventing timing attacks（Elsevier）

主要内容：提出一个运行时检测 / 隔离 / 防止 timing side-channel 攻击的方法（ “Detector”）。在防御部分可引用这一思路。