How do you satisfy the license?

- Include this boilerplate declaration in comment syntax:

- Copyright 2020 Steven Schwab

-

- Licensed under the Apache License, Version 2.0 (the "License");

- you may not use this file except in compliance with the License.

- You may obtain a copy of the License at

-

- http://www.apache.org/licenses/LICENSE-2.0

-

- Unless required by applicable law or agreed to in writing, software

- distributed under the License is distributed on an "AS IS" BASIS,

- WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

- See the License for the specific language governing permissions and

- limitations under the License.

Also include file or class name and description of purpose on the same "printed page" as the copyright notice for easier identification within third-party archives.

What is the actual license of the package and what does it entail?

- The actual license is MIT

- Permission is hereby granted, free of charge, to any person

obtaining a copy of this software and associated documentation

files (the "Software"), to deal in the Software without

restriction, including without limitation the rights to use,

copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the

Software is furnished to do so, subject to the following

conditions:

The above copyright notice and this permission notice shall be

included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT

HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,

WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING

FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR

OTHER DEALINGS IN THE SOFTWARE.

2. Cryptography and signing.

Code the following: Introduce a third party, Charlie. Suppose Alice and Charlie send the message: “Second message” to Bob. Have both Alice and Charlie sign it and Bob verify that they both signed it with code from the lecture.

(Extra Credit: 5 points) Sequential Signing: Have Alice sign a document. Have the signed document signed again by Bob and then have Charlie verify the process.

2a) What is the information that I must always protect in my "wallet"? What is the information Alice and

Charlie have that cannot be sent to Bob?

**Answer:** Must always protect the secret/ private key

4. What is the difference between Encrypting and Digital Signing a Document? (Hint: Look at the cryptography page: https://en.wikipedia.org/wiki/Public-key\_cryptography )

**Answer:** Encrypting makes a digital message attached to a public key which can only be decrypted using a certain private key. Digital signing combines a message with a private key to create a short digital signature on the message. The corresponding public key can be combined with the message and the digital signature to verify if the signature was valid.

4a) What property do all encryption schemes share? They are focused on an operation that is easy to perform yet **hard to factor without any information**. (Hint: Think of multiplying to large prime numbers. This process is easy.)

5. Pretend I have 1M Bitcoins. Why won't the blockchain believe that? The blockchain will not believe that because of the **UTXO** transaction model.

Hint: Source of Answer: https://blockonomi.com/utxo-vs-account-based-transaction-models/