Technische Hochschule Rosenheim
Fakultät für Informatik
Prof. Dr. Reiner Hüttl

IT-Security

Exercise 5

So far, we have used the Standard Library in Java JCE for encryption and digital signatures. With this API you can implement cryptography very individually and fine-grained. However, it is difficult to use for newcomers and non-crypto developers.

Therefore, for comparison, let's look at a crypto API that aims to be easy to use:

The Crypto Library Tink from Google

„Using crypto in your application shouldn't have to feel like juggling chainsaws in the dark. Tink provides secure APIs that are easy to use correctly and hard(er) to misuse.“

Task 0: Check out Google Tink's documentation

https://github.com/google/tink
https://github.com/google/tink/blob/master/docs/Tink-a_cryptographic_library--RealWorldCrypto2019.pdf
https://github.com/google/tink/blob/master/docs/JAVA-HOWTO.md
https://javadoc.io/doc/com.google.crypto.tink/tink/latest/index.html

To use Tink in a Java project, create a Maven project and bind the following dependency into the pom.xml

```
<dependency>
   <groupId>com.google.crypto.tink</groupId>
   <artifactId>tink</artifactId>
   <version>1.7.0</version>
</dependency>
```

Now program the following tasks. The tasks are formulated very freely to give you a lot of options in the implementation.

Task 1: Calculation of a MAC

Calculate a MAC to data of your choice.
Then verify the MAC.

Note: There are HMAC-SHA2 and AES-CMAC in Tink

Task 2: Implement hybrid encryption

Encrypt and decrypt data of your choice with a combination of asymmetric and symmetric encryption.

Note: There are the variants ECIES-AEAD with AES-GCM and AES-CTR in Tink

Task 3: Symmetric encryption with AEAD

AEAD (Authenticated Encryption with Associated Data) is a combination of symmetric encryption and integrity.
Encrypt and decrypt data of your choice.

Note: There are the variants AES-GCM, AES-EAX and CHACHA-POLY1305 in Tink

Task 4: Digital signature

Create and verify a digital signature to data of your choice.

Note: There are the variants ECDSA and RSA in Tink