Programming Project 2023

Carsten Schürmann[*]

April 26, 2023

Preliminaries

For these tasks, we suggest you use Kotlin together with the BouncyCastle library. For an easy setup of your project, you can use either an integrated development engine (like IntelliJ) or the gradle tool. With gradle you can (in a clean directory) start a new project with gradle init, select (2) application as the project type, Kotlin as language, answer the next questions with their defaults and, finally, give your project a name, eg. dk.itu.cryptography. If you have chosen Kotlin as your language, your code will reside in

```
app/src/main/kotlin/dk/itu/cryptography/App.kt.
```

Later on, you can run your project with gradle run in the folder where you created your project. If you have implemented test cases, you can compile and run your tests with gradle check.

Project Description

Alice works at a financial institution and is part of a board authorizing the use of special accounts. Authorization is given if at least three out of the five board members agree on doing so. Since Alice is also working from home currently, she thinks about implementing a digital solution for this authorization. Let's help her by splitting the authorization key into independent shares. Implement the secret sharing scheme by Shamir to split a secret, i.e. a number, into N shares which do not allow to recover the secret unless there are at least k participants cooperating.

For the following tasks, you will use the BouncyCastle library together with Java or Kotlin. Make sure to add the FIPS version 1.0.2 of the library to your project.

- Implement a function to split the secret (represented as a bitstring) into N shares with the polynomial definition from the lecture on a field F and allow reconstruction with at least k shares.

[*] Thanks to Peter Schneider.

- Implement a function to recover the secret out of at least k shares on the field F.
- Test your implementation by reconstructing the secret for the three following shares out of the original five. For each share i, x_i in the polynomial definitions equals i.

```
field =
    00b44a0bc6303782b729a7f9b44a3611b247ddf1e544f8b1
    420e2aae976003219175461d2bd76e64ba657d7c9dff6ed7
    b17980778ec0cbf75fc16e52463e2d784f5f20c1691f17cd
    c597d7a5141080809a38c635b2a62082e310aa963ca15953
    894221ad54c6b30aea10f4dd88a66c55ab9c413eae49c0b2
    8e6a3981e0021a7dcb0759af34b095ce3efce78938f2a2be
    d70939ba47591b88f908db1eadf237a7a7100ac87130b611
    9d7ae41b35fd27ff6021ac928273c20f0b3a01df1e6a070b
    8e2e93b5220ad02104000c0c1e82e17fd00f6ac16ef37c3b
    6153d348e470843a84f25473a51f040a42671cd94ffc989e
    b27fd42b817f8173bfa95bdfa17a2ae22fd5c89dab2822bc
    c973b5b90f8fadc9b074cca8f9365b1e8994ff0bda48b1f7
    498cce02d4e794915f8a4208de3eaf9fbff5
share_0 = ?
share_1 =
    009aca2ca92b1e95bfad348c9014c6adc00d18d29fd5f891
    d0837c9fe18db35cc28d654114d6159dd6664405ead5277e
    24bcdbda9984c28e3b810377744f420e0fc52ada1cafb328
    f6aaa9656d31c73b98af938f784d3d611e7e6f124119e948
    745d15c829d794f47eb76b3fdfc16824ff6d46bcf534b1a2
    d8b3f2de97250f3f3b16f87dba41d54b127c10b2b44d7d54
    c00d89ce91b590c065cc210dd841c8460a7ac535fb0a6e26
    b312695c2635b5a8d311fb4473bee791f35f92dc70524954
    f5f60b98352e4d63b1f8c7357c1e52d696f67b2ff14a988a
    1691352fa0d3401d7d4f806598b651e5e21bc133ad2340a3
    27cef3d47ef2bddc386a98dabcebaa814becb09ce3d8032d
    933664af6b495849030b03e6da89d971e5a45f19ecdef254
    e3549ba5af53ed18b7a013c81b154a06eb76
share_2 =
    2131de2d5f973cd76289fe88dfe2cd9e8196b7cfb26b8793
    fb3afa5bc0b965441878cf300f1a39db3525dc4881a4b465
    4bf648b6b812e202d0ea3e7654fe02cadc68f72978093eee
    3731ecd0ff1f7b32e52de1d9e7575315112cbe693205a089
    0ae8a2fe33610e9097ce3c7f819113315686179c226df4be
    a68cca4e466fcf4ca343fa60019ca4914acedc84df0e12c8
    ad4a3d5590f51e321a7f3528dfb7939241e1377c632e9138
    13ac02757d899a19c10900fdd4ed24d1affc0249b3fdd93d
    f4de4f229dffa039af1589f5fe87cf7594cc8379f364a643
    34ecc165aa650cf81edc2fd1791b95128926c9be25b94e60
    fad290d3f5ef79403025d2ead3ae2f77cc054f4dbc3a5183
    d31eeb8626c00512769ad03092f0b2f256fc2b2f8b62506
    59e656c1569d96b164d7e0908f84e99e728
share_3 = ?
share_4 =
    71da02f27e8f8f82fc996469dc254f81b4db7718ca8bc4fe
    86f6700424c9527db41c2403b69ea80fb2902fa720983929
    691c81b88a7c5bf830b5153d749327b9a80422f2a61cd51b
    5c5c7568a059ab38660f135e05ba62a5e6014d3f0ce4b052
    2b81df3231b111c06199faa7cff0387981dd35cc62ea6a45
    1d2c0b12b39f6676adbe82058c3cb4847856477f8f93962c
    4c10fc5fb62906d95bcb7aad486b564d8c3f50cbeb2d21b6
    aa0e8e46d03b9ba75b1adf4fa9d41ca32e977fbdafadaa4f
    38f20020d30c5f26e30ac1ad56993bc246c06fd0bcbb12e5
    40b1fa6292ba403f45f03f9cf446ac4a37bb4aa180a3f262
    466d3129fccca216c1521143cabc818dda793ce26b3b700c
    3b15cd648193771e797863f7782e6b460d593c92b15a90c8
    43d9d09f65ff1b25cda9b758baa456fe15
```