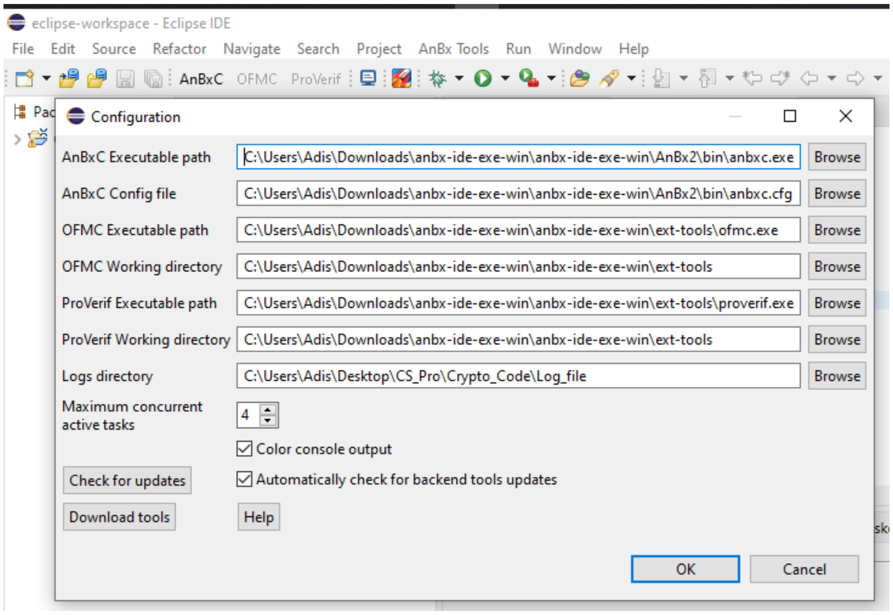
Artifact

The section describes the process to obtain the result with the abstraction of lightweight cryptography using AnBx syntax.

1. Download and installation of Eclipse Integrated Development Environment (IDE) to a local PC as well as Java Mission Control.
2. Installation of Anbx plugin on the Eclipse IDE.


eclipse-workspace - Eclipse IDE
File Edit Source Refactor Navigate Search Project AnBx Tools Run Window Help
AnBxC OFMC ProVerif
Pac
Configuration
Check for updates
Download tools
Help
OK
Cancel

AnBxC Executable path: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\AnBx2\bin\anbxc.exe [Browse]

AnBxC Config file: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\AnBx2\bin\anbxc.cfg [Browse]

OFMC Executable path: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\ext-tools\ofmc.exe [Browse]

OFMC Working directory: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\ext-tools [Browse]

ProVerif Executable path: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\ext-tools\proverif.exe [Browse]

ProVerif Working directory: C:\Users\Adis\Downloads\anbx-ide-exe-win\anbx-ide-exe-win\ext-tools [Browse]

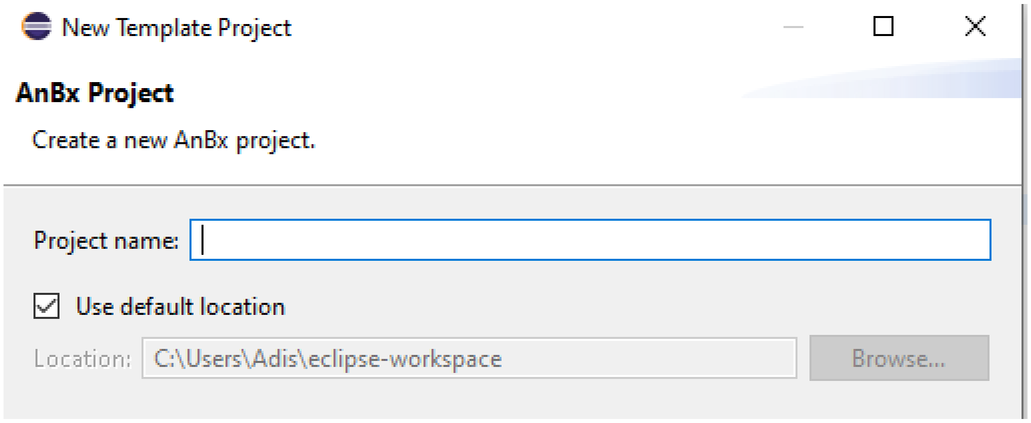
Logs directory: C:\Users\Adis\Desktop\CS_Pro\Crypto_Code\Log_file [Browse]

Maximum concurrent active tasks: 4

☑ Color console output

☑ Automatically check for backend tools updates

3. Create a project folder of AnBx syntax.



AnBx Project

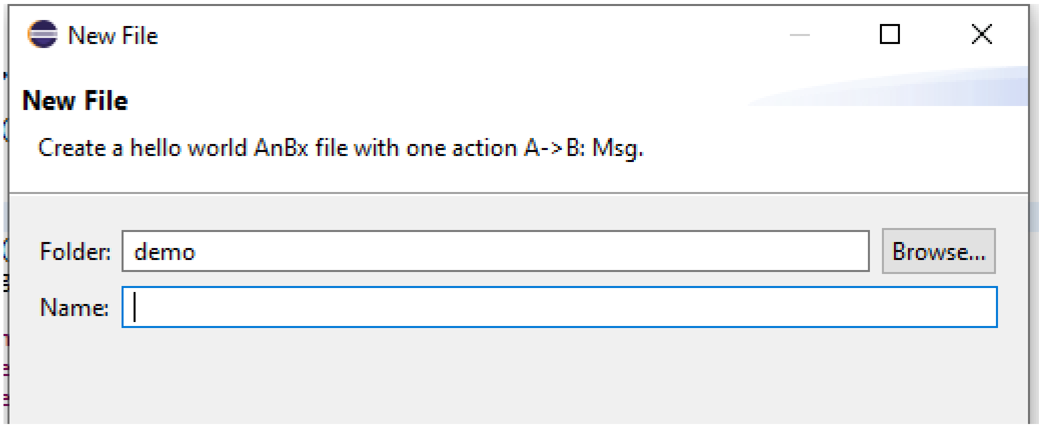
Create a new AnBx project.

Project name:

☑ Use default location

Location: C:\Users\Adis\eclipse-workspace

4. Create AnBx extension file within the AnBx folder.



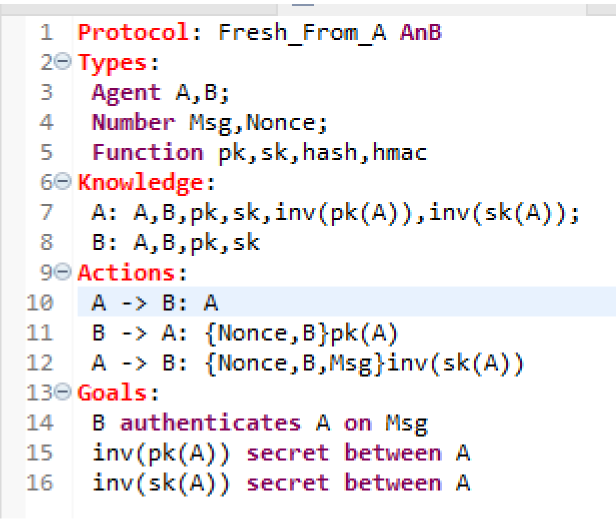
New File

Create a hello world AnBx file with one action A->B: Msg.

Folder: demo

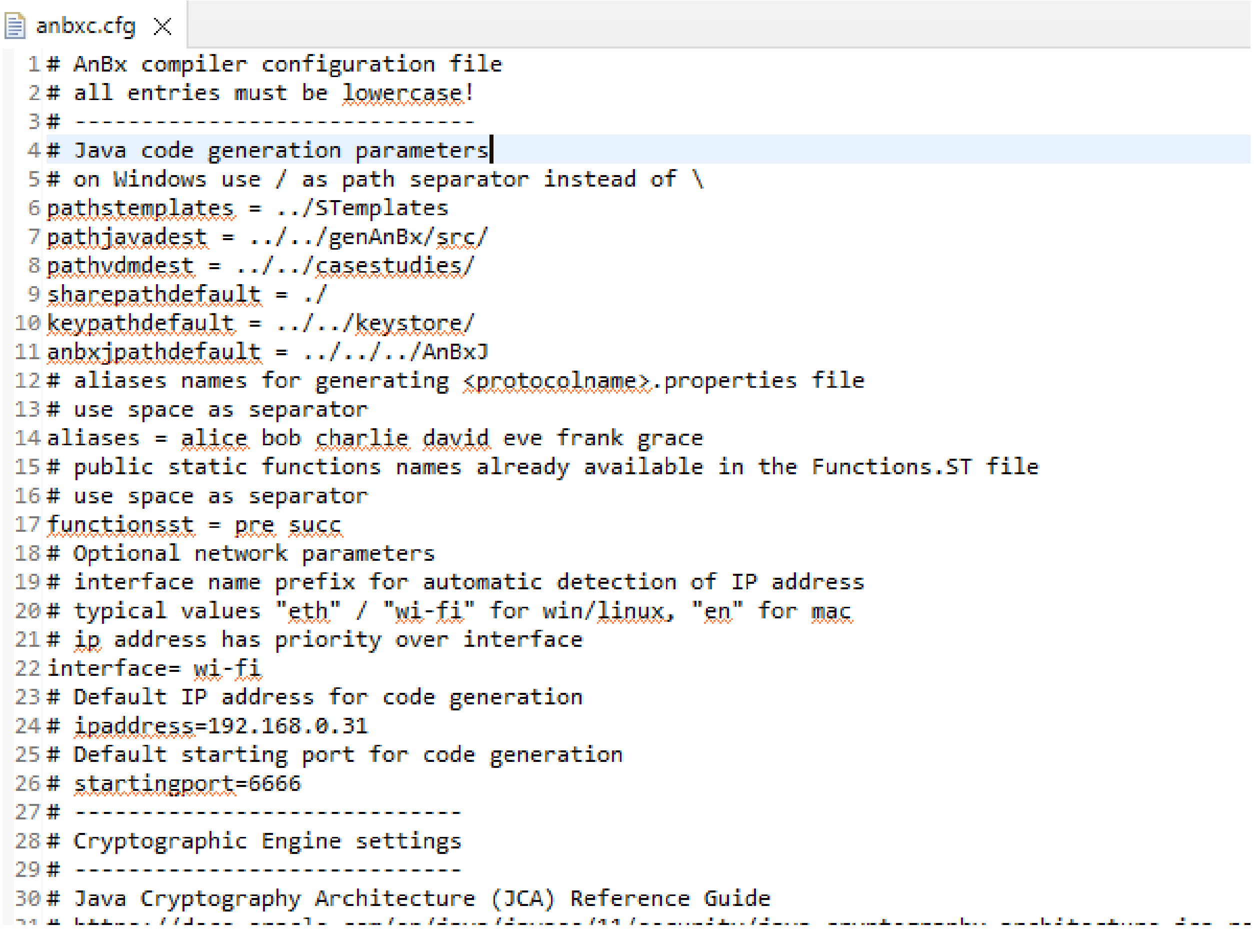
Name:

5. Add any of the selected algorithms to the file.



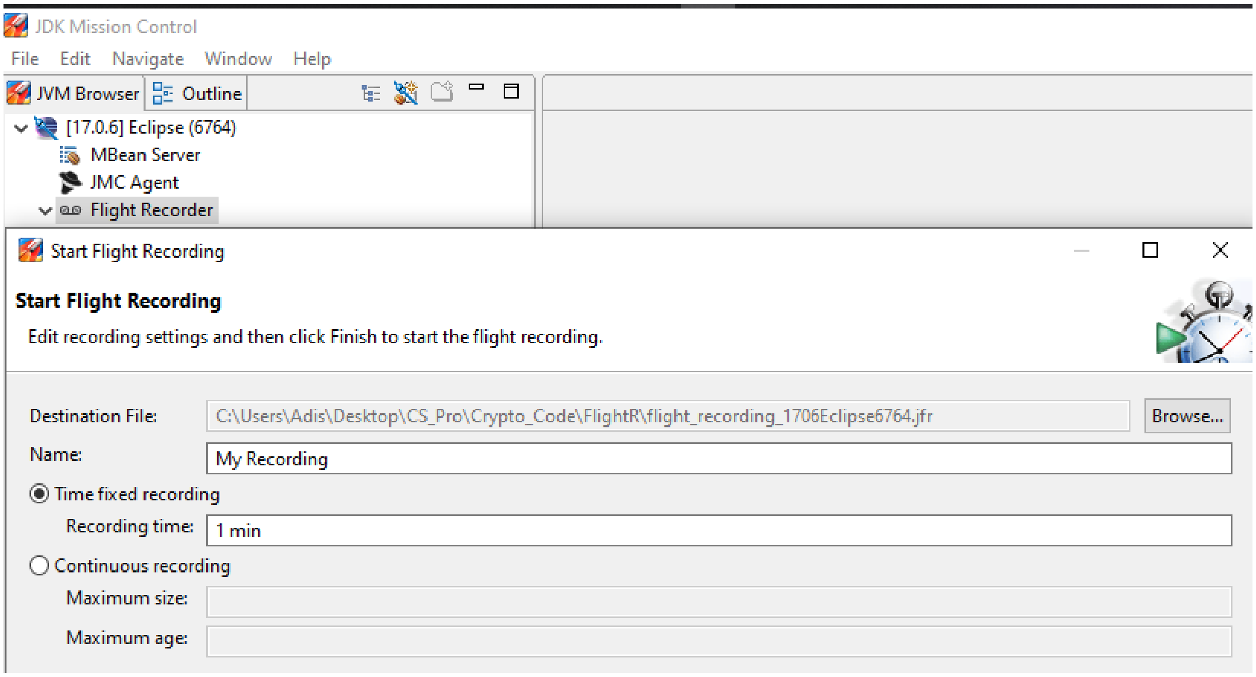
```
Protocol: Fresh_From_A AnB
Types:
 Agent A,B;
 Number Msg,Nonce;
 Function pk,sk,hash,hmac
Knowledge:
 A: A,B,pk,sk,inv(pk(A)),inv(sk(A));
 B: A,B,pk,sk
Actions:
 A -> B: A
 B -> A: {Nonce,B}pk(A)
 A -> B: {Nonce,B,Msg}inv(sk(A))
Goals:
 B authenticates A on Msg
 inv(pk(A)) secret between A
 inv(sk(A)) secret between A
```

6. Modify anbx.cfg to reference the path to keystore, sharepath, and changing of parameters such as key size, key length, secure random algorithm, key pair generation, and cipher algorithms.



```
# AnBx compiler configuration file
# all entries must be lowercase!
# ------------------------------
# Java code generation parameters
# on Windows use / as path separator instead of \
pathstemplates = ../STemplates
pathjavadest = ../../genAnBx/src/
pathvdmdest = ../../casestudies/
sharepathdefault = ./
keypathdefault = ../../keystore/
anbxjpathdefault = ../../../AnBxJ
# aliases names for generating <protocolname>.properties file
# use space as separator
aliases = alice bob charlie david eve frank grace
# public static functions names already available in the Functions.ST file
# use space as separator
functionsst = pre succ
# Optional network parameters
# interface name prefix for automatic detection of IP address
# typical values "eth" / "wi-fi" for win/linux, "en" for mac
# ip address has priority over interface
interface= wi-fi
# Default IP address for code generation
# ipaddress=192.168.0.31
# Default starting port for code generation
# startingport=6666
# -----------------------------
# Cryptographic Engine settings
# -----------------------------
# Java Cryptography Architecture (JCA) Reference Guide
# https://docs.oracle.com/en/java/javase/11/security/java-cryptography-architecture-jca-re
```

7. Start a flight record on JMC as applied to Eclipse server.



Start Flight Recording

Start Flight Recording

Edit recording settings and then click Finish to start the flight recording.

Destination File: C:\Users\Adis\Desktop\CS_Pro\Crypto_Code\FlightR\flight_recording_1706Eclipse6764.jfr

Name: My Recording

● Time fixed recording

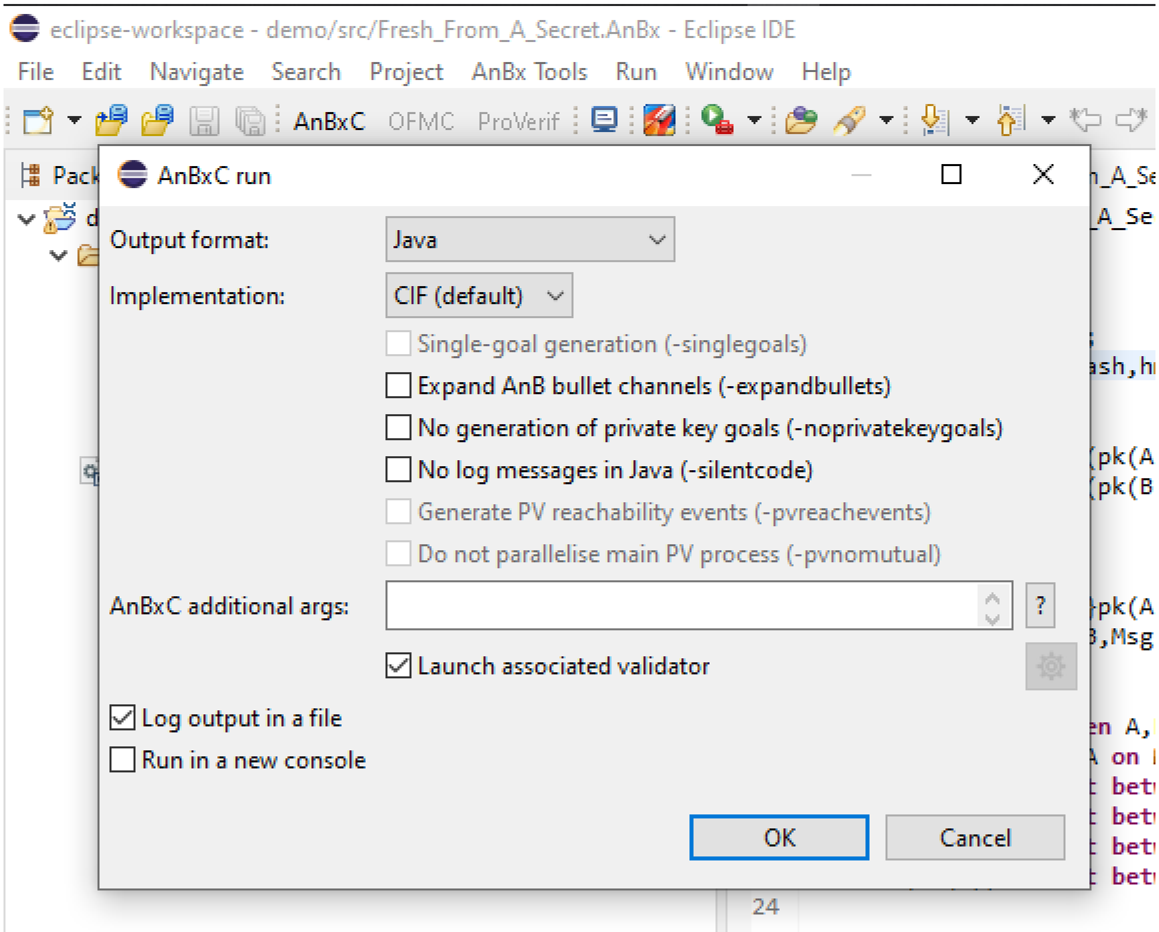
Recording time: 1 min

○ Continuous recording

Maximum size:

Maximum age:

8. Start the flight record.
9. Run the algorithm or protocol on Eclipse.


eclipse-workspace - demo/src/Fresh_From_A_Secret.AnBx - Eclipse IDE
File Edit Navigate Search Project AnBx Tools Run Window Help
AnBxC OFMC ProVerif
AnBxC run
OK
Cancel

Output format: Java

Implementation: CIF (default)

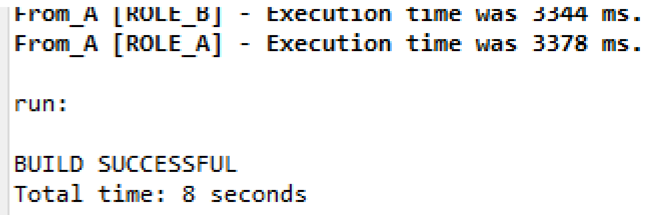
□ Single-goal generation (-singlegoals)
□ Expand AnB bullet channels (-expandbullets)
□ No generation of private key goals (-noprivatekeygoals)
□ No log messages in Java (-silentcode)
□ Generate PV reachability events (-pvreachevents)
□ Do not parallelise main PV process (-pvnomutual)

AnBxC additional args:

☑ Launch associated validator

☑ Log output in a file
□ Run in a new console

10. Stop the flight record after the complete execution of Eclipse.
11. Take computation time and execution time from Eclipse.

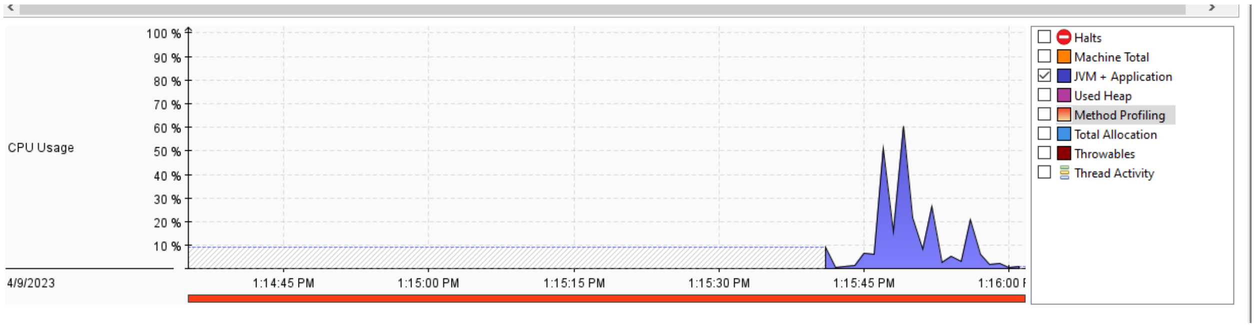


```
From_A [ROLE_B] - Execution time was 3344 ms.
From_A [ROLE_A] - Execution time was 3378 ms.

run:

BUILD SUCCESSFUL
Total time: 8 seconds
```

12. Record CPU usage from JMC.



☐ Halts
☐ Machine Total
☑ JVM + Application
☐ Used Heap
☐ Method Profiling
☐ Total Allocation
☐ Throwables
☐ Thread Activity