23/10 Eclipse with Java Card 3.0.5 JDK, OpenCard

28/10 Wrote skeleton OpenCard code

31/10 Reader arrived. Used gpshell to load example applet to card, list card applets, remove applet. Attempted to load my own test applet, realised that 3.0.5 applet is not compatible. Purchased 3.0.4 cards because of easier dev process (eclipse plugin) and better library.

4/11 Attempted to run sample project with OCF. OCF wouldn’t recognise the card. Identified that OCF requires reader has OCF driver but it only has PC/SC driver. (find source). Reader data sheet only specifies PC/SC but some readers also specify OCF. OCF programmer’s guide: “The OpenCard Reference implementation comes with a lockable CardTerminal implementation for PCSC card readers”. Reference implementation contains classes that appear to translate.

Noticed new cards are 3.0.4 and not 3.0.5 compatible.

5/11 Chose pyscard Python library instead of OCF. Wrote test program to select applet using SELECT APDU with the ISD, prints status words.

7/11 Environment variable trouble, partly due to distributer. Compiled, converted and uploaded my own applet.

11/11 Set up Atom with Python and Java IDEs. Wrote applet to take data string, store, and return later.  
Wrote script to compile, convert, upload, run.

14/11 Chose OPACITY, researched relevant aux functions, python crypto libraries

18/11 Wrote helper functions for card and host.

23/11 Wrote CMAC because not implemented on 2.2.2. Wrote initial Opacity implementation. Cast everything to short.

3/12 implemented ecdh, kdf, signature.

9/12 JCMathLib problems tried to compile as separate library but wouldn’t work. Depended on static arrays which can’t be used in JC libraries, and if it were a full package it doesn’t present an API to other packages. However, 64KB package limit needs to be observed. copied source into main package.

15/12 Mod\_inv (used in ecdsa) fails, error in library, implemented myself.

Couldn’t perform TLV ops with 2.2.2 library because they were in javacardx package, not implemented.

Performed static array allocation during each execution, repeated executions caused memory overflow. requestObjectDeletion() solved it.

Bug in jcmathlib. Didn’t appear to be properly releasing locks on objects so had to disable object locking.

18/12 More work on host end, bug fixing etc.

19/12 Implemented incorrect ECDH impl. Fixed CMAC bugs. Works, time taken is 2.9s.

24/12 For host “cryptography” library to take card pubkey and deserialise to its pubkey object type, it needs DER structure defined in RFC5280. Defines full certificate, not relevant. Decided to do myself.

28/12 ecdh being wrong on card caused headache. CMAC bug fixes

2/1/2018 Fixed ecdh on host by using proper \*/+ operators of EC points using a library “rubenesque”. Others tend to use GMP (GNU Multiple Precision Arithmetic Library) for EC stuff or are very slow.

JC KeyAgreement (ecdh) causing problems because it returns sha-1 hash instead of multiplication result.

3/1 JCMathLib point\_mult not working. Attempted to implement my own. Had to write mov\_inv, which I needed an egcd auxiliary function for, but it kept failing at a Bignat multiplication on the 12th pass. Killed all my cards.

14/1 Wrote my own BigInt to simplify and fix bugs, now it fails on 13th pass. Appears that 2 consecutive failures brick the card. This bug killed 6 JC 2.2.2 cards at a cost of about £25, and I wasn’t making progress. “I can’t continue like this”. Decided to switch to the 3.0.4 cards.

16/1 Build C-R test project on 3.0.4 card, then built main applet, using ANT tasks. Still problem with egcd, but not card-breaking, again due to repeated calls to mod\_mult. JCMathLib INVALIDCOPYOTHER exception. Did various other work on ecdsa.

19/1 Kuhn responded wrt. The KeyAgreement stuff, telling me it was due to hashing the secret. Old library only allowed hashed output, new 3.0.4 library also allowed unhashed ECDH output.

Couldn’t use ALG\_AES\_MAC\_128\_NOPAD for CMAC because not supported. Used 128b CBC instead, taking last 16b.

21/1 began implementing PB. Identified error in the standard at C13.

30/1 Another standard bug. Host-end, S2. If host wants to suppress PB but a record exists, host will still do PB lookup in later part. Finished implementing optimised version. Emailed author about errors, no reply.

16/2 bug fixes in cmac stuff.

17/2 took timing measurements, made optimisations, took more measurements.