Verificarea Monocypher cu FramaC/Eva

Adrian Manea

Cuprins

DE ADĂUGAT SAU CLARIFICAT

INTRODUCERE

Proiectul prezentat este `Monocypher` (LoupVaillant (2019a)), care este o bibliotecă criptografică scrisă de Loup Vaillant, începînd cu 2016. După cum menționează autorul pe pagina LoupVaillant (2017), intenția a fost de a concepe o bibliotecă de criptare suficient de sigură, de rapidă, dar și de simplă pentru a fi folosită atît de el, cît și de alții. Autorul a considerat că bibliotecile actuale ori nu sînt suficient de sigure, ori sînt supraîncărcate pentru necesitățile sale, așa că a pornit în a-și concepe propria soluție. Proiectul este scris în C.

Verificarea proiectului `Monocypher` se va face folosind pachetul `FramaC` (Baudin (2019)), specific pentru limbajul C. Cum `FramaC` este, de fapt, mai curînd un mediu în care se pot rula mai multe unelte de verificare formală, am ales verificarea `Monocypher` cu `Eva`.

Detaliile despre modul de funcționare a proiectului `Monocypher`, cît și a verificării prin `Eva` sînt date în secțiunile următoare.

BIBLIOGRAFIE

Baudin, P. h. (2019). `FramaC`. site oficial. online, accesat aprilie-mai 2019.

FramaC, G. (2019). `Eva`. manual oficial. online, accesat aprilie-mai 2019.

LoupVaillant (2017). How i implemented my own crypto. eseu online. online, accesat aprilie-mai 2019.

LoupVaillant (2019a). `Monocypher`. GitHub. online, accesat aprilie-mai 2019.

LoupVaillant (2019b). `Monocypher`. site oficial. online, accesat aprilie-mai 2019.

Wikipedia (2019). Abstract interpretation. link. online, accesat aprilie-mai 2019.