Secure Applications Programming Resources
Exam – 3 Feb 2014

Să se scrie aplicația consolă Java sau C++ care decriptează cifrul stocat în fișierul *Msg.enc* utilizându-se:

Fișierul ***ISMCertificateX509.cer*** (pt. soluție Java) sau ***pubISM.pem*** (pt soluție C++) ce conține o cheie publică RSA pe 1024 biți

Fișierul ***key.sec*** (varianta Java sau C++) ce conține o cheie AES pe 128 biți criptată cu cheia privată RSA, perechea celei din certificat

Fișierul ***Msg.enc*** (varianta Java sau C++) ce conține un mesaj criptat AES în mod CBC cu padding PKCS5 (pt. soluția Java) sau fără padding (pt. soluția C++). Primii 128 biți din fișierul ***Msg.enc*** reprezintă **IV-ul** în clar.

Aplicația consolă:

10p – afișează cheie AES în clar ca string;

20p – generează fisier ***Msg.txt*** ce conține textul decriptat

20p – afișează hash MD5 calculat pentru ***Msg.enc***