Secure Applications Programming Resources
Exam – 2 February 2015

Să se scrie aplicația consolă Java care decriptează cifrul stocat în fișierul ***mesaj.aes*** utilizându-se:

Un dicționar de parole ***hak5.txt*** ce conține cheia de acces a keystore-ului ***examkeystore.ks***.

Valoarea hash din fișierul ***pass-hash.txt*** corespunzătoarea parolei corecte din fișierul *hak5.txt*.

Fișierul ***ISMCertificateX509.cer*** (pt. soluție Java) ce conține o cheie publică RSA pe 1024 biți

Fișierul ***AESKey.sec*** (varianta Java) conține o cheie AES pe 128 biți criptată cu cheia publica RSA, perechea intrării *examkey2* din keystore-ul *examkeystore.ks*

Fișierul ***mesaj.aes*** (varianta Java) ce conține un mesaj criptat AES în mod CBC cu padding PKCS5 (pt. soluția Java). **IV-ul** are valoarea 0000000….000 si este cunoscut la criptare/decriptare fără a fi salvat in fișier.

Aplicația consolă:

10p – afișează cheia din dicționarul *hak5.txt* corespunzătoarea valorii *hash* din fișierul ***pass-hash.txt***;

20p – afișează cheia AES in clar ca String. Valoarea cheii este stocata criptata in fișierul ***AESKey.sec*** cu cheia publica RSA a intrării *examkey2*

20p – generează fișierul text decriptat pentru ***mesaj.aes***