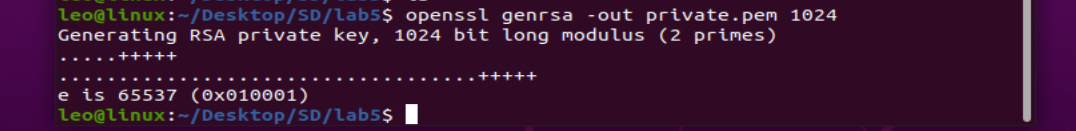
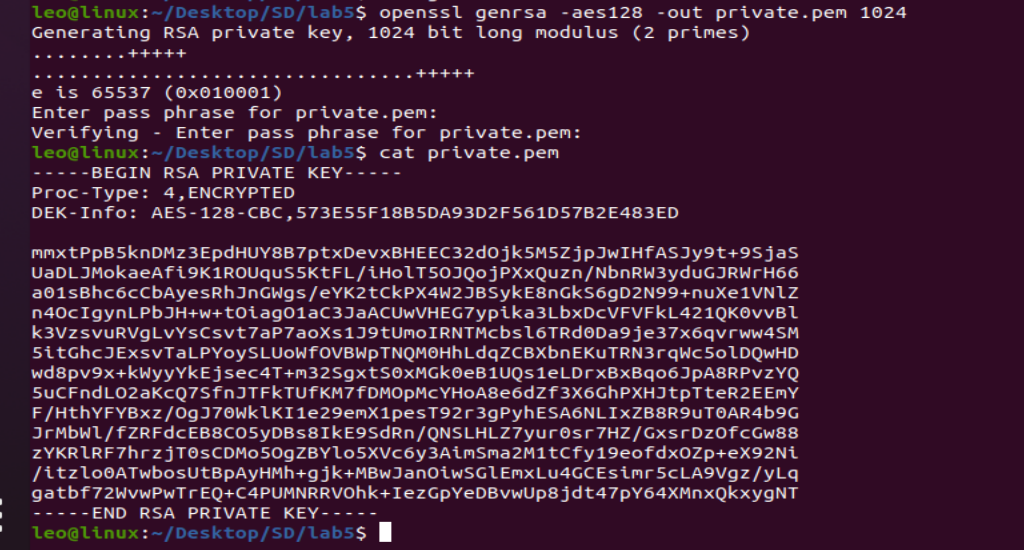
1. (1p) Generati o cheie de 1024 biti: *openssl genrsa -out private.pem 1024*

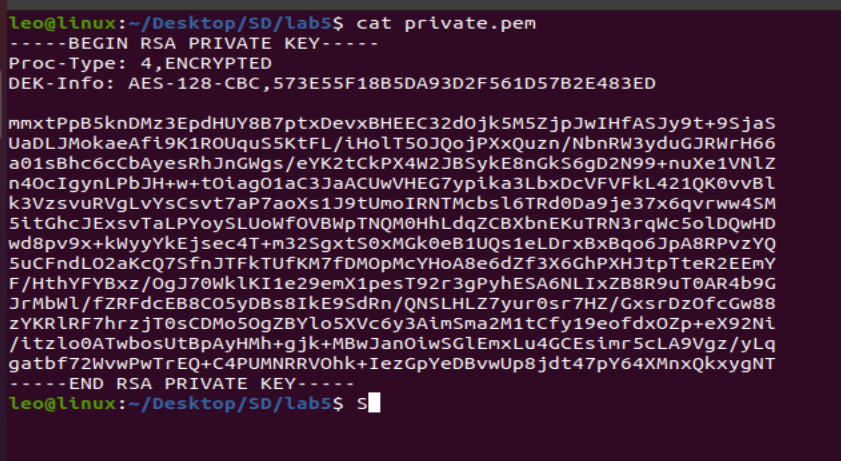


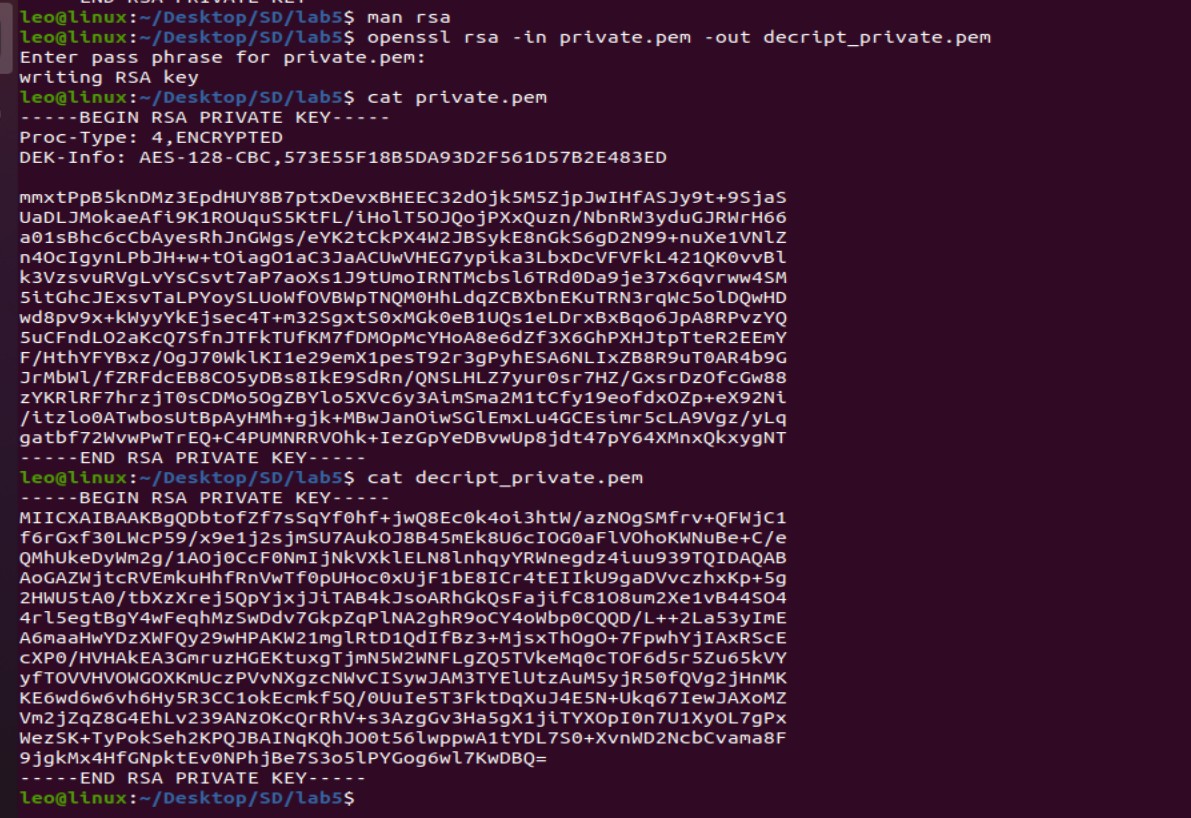
1. (1p) Oricine intră în posesia fişierului private.pem poate utiliza cheia pentru criptarea şi decriptarea mesajelor. Pentru a împiedica utilizarea cheii private de către un potenţial intrus care intră în posesia ei se impune protejarea acesteia cu parolă. Securizarea se face criptând cheia privată folosind un algoritm cu cheie simetrică. Pentru a afla mai multe amănunte parcurgeţi secţiunea genrsa din manualul openssl (tastaţi *man genrsa*). Rescrieţi comanda anterioară astfel încât să generaţi o cheie criptată; precizaţi algoritmul folosit pentru criptarea cheii.

Am folosit Aes-128

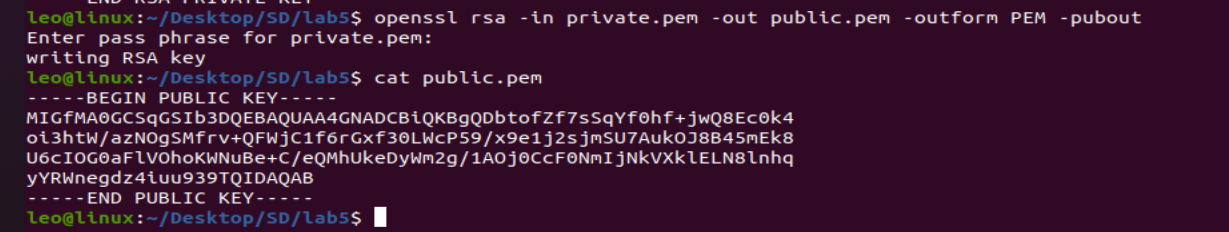


1. (2p) Este posibilă şi criptarea unei chei deja existente (care nu a fost criptată), precum şi înlăturarea criptării pentru o cheie criptată (vezi man rsa). Scrieţi comenzile pentru criptarea şi respectiv înlăturarea criptării pentru o cheie existentă corespunzătoare. Afişaţi conţinutul fişierului private.pem pentru situaţia când acesta nu este criptat iar apoi afisaţi continutul fiţierului când acesta este criptat



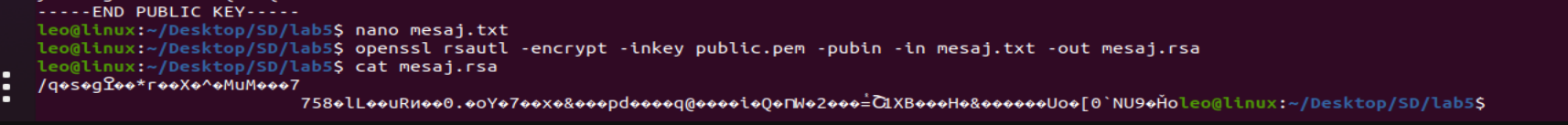


1. (1p) Fişierul private.pem creat la pct .1 conţine practic atât cheie privată cât şi pe cea publică, deci nu-l putem pune la dispoziţia interlocutorului. Pentru a extrage cheia publică procedaţi astfel: *openssl rsa -in private.pem -out public.pem -outform PEM -pubout.*În acest moment puteţi distribui fişierul public.pem care reprezintă cheia voastră publică către oricine doriţi. Este posibilă extragerea cheii private din fişierul public.pem?

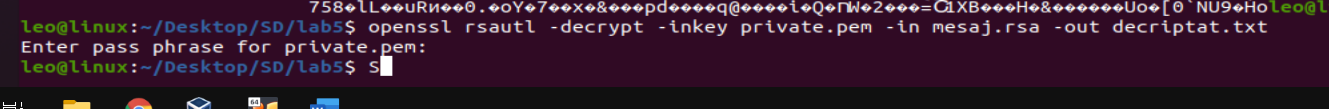


Nu este posibila extragerea cheii private din fisierul public.pem deoarece in public.pem se afla doar cheia publica

1. (1p) Criptati fişierul mesaj.txt (create anterior de voi cu un continut text): *openssl rsautl -encrypt -inkey public.pem -pubin -in mesaj.txt -out mesaj.rsa.*Afişaţi conţinutul fişierului mesaj.rsa.



1. (1p) Folosind cheie privată puteţi decripta fişierul: *openssl rsautl -decrypt -inkey private.pem -in mesaj.rsa -out decriptat.txt.*Vi s-a solicitat o parolă? Dacă da în ce condiţii, dacă nu în ce condiţii? Cum contribuie parola la decriptarea fişierului mesaj.rsa?



Da a solicitat introducerea parolei in conditiile in care am introdus-o la crearea cheii. Presupun ca pentru a decripta mesaj.rsa trebuie accesata cheia privata din cadrul fisierului private.pem, nu se poate face acest lucru fara a introduce parola.

1. (3p) În cadrul acestei activităţi va trebui să studiaţi performanţa algoritmilor cu cheie publică. Pregătiţi un fişier (mesaj.txt) ce conţine un mesaj de 16 octeţi. Generaţi o pereche de chei publică/privată de 4096 de biţi (private4096.pem / public4096.pem), 1024 (private1024.pem / public1024.pem) şi 512 de biţi (private512.pem / public512.pem). Nu criptaţi cheile! Folosind fiecare pereche de chei efectuaţi următoarele operaţii: 1. criptaţi mesaj.txt folosind cheie publică; salvaţi rezultatul în mesaj.rsa 2. decriptaţi mesaj.rsa folosind cheia privată. De fiecare dată obţineţi timpul necesar procesului de criptare şi decriptare prin folosirea comenzii time (adunaţi user şi sys). Criptaţi mesaj.txt folosind AES cu cheie pe 128 de biţi, apoi decriptaţi-l. Înregistraţi şi în acest caz timpul necesar procesării. Completaţi intr-un tabel de forma:

                                  AES128               RSA512                RSA1024                 RSA4096

Timp Criptare

Timp Decriptare

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | AES128 | RSA512 | RSA1024 | RSA4096 |
| Timp Criptare | 0.004s | 0.003s | 0.003s | 0.003s |
| Timp Decriptare | 0.004s | 0.004s | 0.004s | 0.011s |

