



# Examen SSI

Data 26.01.2022

Nume: Horjea Cosmin-Marian

Grupa 343

Subiecte Netratate: 3(c,d)

2 2 2 0 2 0 2 0 0 0 2 5 5 5 2 0 0 5

1.

- a. Fals. Decriptarea, folosind OTP, a textului criptat 0x253505ba folosind cheia 0x717056ee este mesajul clar TEST ●
- b. Adevarat ●
- c. Adevarat ●
- d. Adevarat ●
- e. Fals. Este recomandat sa se foloseasca RSA pentru transmiterea cheilor in mod criptat ●
- f. Adevarat ●
- g. Fals. SHA256(PAR123) = 467b4a3eca61a4e62447400d93fc35d4295c08ffa2b04ae942f4de03fa62f464 ●
- h. Adevarat ●
- i. Adevarat ●
- j. Adevarat ●

2.

- a. Principle of diversity deoarece se folosesc mai multe tipuri de algoritmi criptografici precum AES-ECB, TLS, CRC, functii hash. ●
- b. Se incalca principiul lui Kerckhoffs care spune ca totul, exceptand cheile criptografice, ar trebui sa fie publice, iar functia hash din exemplu este proprietara si nu ni se ofera acces la implementarea acesteia ●
- c. Integritatea datelor este supusa riscului deoarece codul CRC atasat mesajelor din aplicatie poate fi recalculat pentru mesajul alterat de catre un adversar activ si atasat inapoi mesajului, iar confidentialitatea este si ea precara deoarece criptarea fisierelor condifentiale este facuta cu modul ECB care este stiut ca nu este sigur ●
- d. Un exemplu poate fi acesta:
  - cunoastem adresa de email a unui utilizator
  - am putea sa incercam sa-i schimbam parola
  - stim ca generarea linkului parolei este facuta cu un sistem PRNG care foloseste ca seed usernameul si ziua curenta
  - Cu un seed atat de predictibil putem sa generam un link de resetarea al parolei destul de usor ●

3.

- a. Ca sa verificam ca un o semnatura  $\sigma$  este valida, ridicam la puterea  $e$  care face parte din cheia publica, avem:

$\sigma^e = ((m')^d)^e$ , stim ca  $d = e^{-1}$  ceea ce ne rezulta  $((m')^{e^{-1}})^e$  ceea ce ne da  $m'$  deci stim ca e o semnatura valida ●

- b. stim  $\sigma = (m')^d$ , daca incercam sa validam semnatura din  $(2m, 2^d\sigma)$  calculam:

$$(2^d\sigma)^e = (2^d(m')^d)^e = (2^d)^e \cdot ((m')^d)^e = (2^{e^{-1}})^e \cdot ((m')^{e^{-1}})^e = 2m'$$

Ca semnatura sa fie valida ar fi trebuit sa obtinem  $(2m)'$ , dar avem  $2m'$

stim ca operatia de  $2x$  pe biti ar rezulta in  $x||0$

notam paddingul din enunt cu *pad*

$$(2m)' = (2m')$$

$$(m||0)' = 2(pad||m)$$

$$(pad||m||0) = (pad||m||0)$$

⇒ semnatura este valida 🟡

c.

d.

4. MAC-ul de specificat nu este sigur,

Daca alegem orice mesaj  $m$  cand evaluam expresia  $m \text{ AND } NOT(m)$  o sa avem mereu un sir lung de 0

Practic daca alegem doua mesaje  $m_1$  si  $m_2$  ,  $|m_1| = |m_2| = n$ ,

$m_1 \neq m_2$  si incercam sa aplicam  $Mac'$  pe acestea vom avea:

$$Mac'(k, m_1) = Mac(k, m_1 \text{ AND } NOT(m_1)) = Mac(k, 0^n) = T_1$$

$$Mac'(k, m_2) = Mac(k, m_2 \text{ AND } NOT(m_2)) = Mac(k, 0^n) = T_2$$

$T_1 = T_2$  deci orice mesaje de aceeasi lungime au acelasi tag

Ceea ce inseamna ca un atacator poate sa modifice un mesaj si sa-i calculeze tag-ul atat timp cat ii stie lungimea 🟢