Securitatea Sistemelor Informatice - Restanţă: 3 mai 2022

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **4 mai, ora 10:00**.
   - Transmiterea corectă a examenului este strict în responsabilitatea studenţilor.
   - Transmiteţi în timp util, NU aşteptaţi ultimele minute pentru a încărca examenul. Examenul poate fi transmis de oricâte ori doriţi până la deadline, se ia în considerare doar ultima variantă transmisă. NU se acceptă ca motivaţie pentru netransmiterea examenului niciun fel de probleme tehnice (încetinirea platformei, utilizarea incorectă, nesincronizări ale ceasului platformei, etc.).
   - Studenţii care nu transmit rezolvarea examenului scris sunt consideraţi absenţi.
2. Răspunsul trebuie să fie în **format .pdf, încărcat prin contul instituţional Moodle** în secţiunea corespunzătoare sub numele **grupa_nume_prenume.pdf**. Prima pagină a fişierului de răspunsuri trebuie să conţină **nume, grupă, o listă a subiectelor netratate** (ex.: *Subiecte netratate: 1(a), 1(c), 3(b).* sau -).
   - Este la latitudinea fiecărui student cum redactează examenul: scan al foilor scrise de mână (citeţ / lizibil!), Word / LaTeX exportat în pdf, etc.
   - Aveţi grijă ca fişierul final .pdf să fie valid şi rezolvările să fie uşor identificabile!
3. Se acordă punctaje parţiale. Răspunsurile greşite la examenul scris NU depunctează suplimentar.
4. Pentru promovare, **este obligatoriu să participaţi la ambele probe (examen scris şi oral), să obţineţi minim 10 puncte la examenul final şi minim 45 de puncte** ca notă finală (include punctele obţinute în timpul anului).
5. Pentru examenul oral:
   - Este strict în responsabilitatea studenţilor să verificaţi repartizarea pe zile / ore (aprox.) şi alte informaţii necesare referitoare la susţinerea examenului oral.
   - Trebuie să vă conectaţi **audio-video, folosind contul instituţional Teams**.
   - Trebuie să arătaţi **un act de identitate**, de preferat **legitimaţie / carnet de student cu poză**. Este în responsabilitatea studenţilor să ascundeţi alte informaţii (altele decât numele şi poza) de pe documentul prezentat, pe care nu doriţi să le faceţi publice!
   - Fiecare subiect rezolvat în scris, dar pe care nu ştiţi să îl explicaţi (i.e., să arătaţi că l-aţi rezolvat individual sau înţeles), **se depunctează cu dublul punctajului alocat subiectului respectiv**.
   - Studenţii care transmit rezolvarea examenului scris dar nu participă la susţinerea orală obţin nota finală 4.
   - Dacă există studenţi care nu au posibilitatea unei conexiuni audio şi video, trebuie să anunţe în prealabil, pe e-mail (*adela@fmi.unibuc.ro*).

Dacă în timpul examenului aveţi întrebări, le puteţi posta pe forum, secţiunea *Examen*. Urmăriţi formul pentru informaţii. **NU postaţi indicii sau soluţii!**

SUCCES!

EXAMEN ONLINE - Probleme

1. **Adevărat sau Fals**

   Răspundeţi cu adevărat sau fals. Dacă afirmaţia este falsă, transformaţi-o într-o afirmaţie adevărată printr-o schimbare minimală (i.e., păstraţi contextul, dar nu negaţi). Subliniaţi modificarea adusă.

   Exemplu: RSA este un sistem de criptare simetric.
   Răspuns: Fals. RSA este un sistem de criptare ***asimetric****.*

   (a) Decriptarea, folosind OTP, a textului criptat 0x475853464959 folosind cheia 0x43415354454c este mesajul clar SISTEM. **(2p)**

   (b) Rolul codurilor de autentificare a mesajelor este să asigure confidenţialitatea mesajelor. **(2p)**

   (c) In cadrul sistemului de criptare OTP se pot cripta mai multe mesaje cu aceeaşi cheie, trebuie doar ca lungimea cheii să fie cel puţin la fel de mare ca lungimea mesajului. **(2p)**

   (d) Criptarea cu cheie publică este semnificativ mai rapidă decât criptarea cu cheie privată. **(2p)**

   (e) Metoda de încercare-şi-eroare prin care se încearcă decriptarea datelor criptate printr-un efort exhaustiv în locul folosirii unui efort intelectual şi al unor tehnici specifice se numeşte criptanaliză. **(2p)**

   (f) Schimbul de chei Diffie-Hellman este vulnerabil la un atac de tip phishing iar securitatea lui se bazează pe problema computaţională Diffie-Hellman. **(2p)**

   (g) Pincipala componentă a unui sistem de criptare fluid este un PRG. **(2p)**

   (h) SSL/TLS implementează principiul diversităţii pentru că permite alegerea unor sisteme de criptare diferite pentru a fi folosite în aceeaşi etapă (ex. pentru transmiterea criptată). **(2p)**

   (i) Problema care sta la baza criptografiei pe curbe eliptice este problema factorizării numerelor mari. **(2p)**

   (j) Pentru evitarea atacurilor cu text criptat ales împotriva RSA, se recomandă folosirea variantei OAEP. **(2p)**

2. Sunteţi angajat să verificaţi securitatea în cadrul unei companii. Observaţi că se folosesc următoarele:

   - Sistemul de criptare DES în modul CTR pentru stocarea criptată a fişierelor.
   - AES pentru stocarea parolelor clienţilor cu *salt*.
   - Protocolul de schimb de chei Diffie-Hellman autentificat pentru generarea cheilor necesare securizării comunicaţiei interne (i.e., între angajaţii firmei) într-un grup pentru care un adversar PPT poate rezolva Problema decizională Diffie-Hellman cu o probabilitate $\lambda(n) = 1/3^n$, unde n este parametrul de securitate.
   - Site-ul web al companiei este securizat folosind certificate digitale cu modulul RSA N pe 4096 de biţi.

- Integritatea end-to-end a mesajelor m transmise în modulul de chat (folosit pentru comunicarea în cadrul companiei) este asigurată de codul de autentificare a mesajelor HMAC(m), a cărui valoare se apendează mesajului transmis.
- Pentru minimizarea numărului de chei stocate, se foloseste aceeaşi cheie secretă pentru criptarea fisierelor stocate (pentru DES) şi pentru HMAC.

Răspundeţi la următoarele cerinţe:

(a) Sunt parolele clienţilor stocate în mod sigur? Argumentaţi. (1 paragraf) **(2.5p)**

(b) Ce puteţi spune despre securitatea sistemului RSA folosit în cadrul certificatelor digitale? (1 paragraf) **(2.5p)**

(c) Ce puteţi spune despre funcţia λ şi securitatea schimbului de chei Diffie-Hellman? (1 paragraf) **(5p)**

(d) Enunţaţi un principiu de securitate (referiţi-vă la *Pages on Security - Principles*) care este NU este satisfăcut. Argumentaţi. (1 paragraf) **(5p)**

(e) Există probleme de securitate (confidenţialitate, integritate) la nivelul aplicaţiei? Argumentaţi. (1 paragraf) **(5p)**

3. Se consideră modul de operare definit mai jos pentru criptarea unei secvenţe de blocuri $m_1||m_2||m_3||\ldots$ într-o secvenţă de blocuri $c_1||c_2||c_3||\ldots$:

$$c_i = m_i \oplus F_k(m_{i-1} \oplus c_{i-1}), i \geq 1$$

unde m_0 şi c_0 sunt vectori de iniţializare publici şi fixaţi.

(a) Ce reprezintă notaţia F_k? Ce proprietate esenţială trebuie să satisfacă funcţia F_k pentru ca sistemul să fie corect?**(2 $\times$ 2.5p)**

(b) Indicaţi cum se realizează decriptarea. **(5p)**

(c) Câte valori posibile pot lua m_0 şi c_0 dacă sunt reprezentate fiecare pe 16 biţi? Ce puteţi spune despre securitatea sistemului în acest caz? **(2 $\times$ 2.5p)**

(d) Presupunând că un bloc c_i suferă erori de transmisie, care blocuri de text clar sunt impactate? **(5p)**

4. Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ şi $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentaţi răspunsul. **(5p)**

$Mac'(k,m) = Mac(k,m)$

$$Vrfy'(k,m,t) = \begin{cases} Vrfy(k,m,t), & \text{dacă } m \neq 0^n \\ 1, & \text{altfel} \end{cases}$$

TOTAL disponibile: 65p