Securitatea Sistemelor Informatice - Examen: ianuarie 2022

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **27 ianuarie, 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 (*ruxandra.olimid@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 0x253505ba folosind cheia 0x717056ee este mesajul clar MARE. **(2p)**

   (b) Niciun sistem determinist nu poate fi CCA-sigur. **(2p)**

   (c) Un atac de tip Man-in-the-Middle este un atac activ. **(2p)**

   (d) Un PRP presupune ca pentru fiecare intrare, ieşirea să conţină exact biţii de intrare, permutaţi presudoaleator (ex. pentru o cheie fixată K şi $PRP_K : \{0,1\}^4 \to \{0,1\}^4$, $PRP_K(1101) = 1011$ poate fi o atribuire corectă dar $PRP_K(1101) = 0101$ este întotdeauna o atribuire incorectă). **(2p)**

   (e) Este recomandat să se folosească RSA pentru transmiterea fişierelor în mod criptat. **(2p)**

   (f) Pentru a asigura integritatea unor fişiere personale, este suficient să stocaţi pe calculatorul propriu fişierele şi valoarea SHA256 corespunzătoare fiecăruia sub forma *(file1,SHA256(file1))*, *(file2,SHA256(file2))*. .... **(2p)**

   (g) SHA256(PAROLA) = 0x1c65fc11a8651621 765d50083695b33b 4de0d253ff984adb 62f64e4c0504ed1f. **(2p)**

   (h) Scopul principal al unui adversar împotriva schimbului de chei Diffie-Hellman este să spargă Problema Logaritmului Discret (PLD). **(2p)**

   (i) Faptul că majoritatea certificatelor digitale bazate pe RSA folosesc exponentul de criptare = 65537 nu este o problemă de securitate dacă valoarea factorilor p şi q este întotdeauna mare. **(2p)**

   (j) SSL/TLS implementează principiul diversităţii (*principle of diversity*) pentru că foloseşte în *handshake protocol* criptografia asimetrică (ex. certificate pentru autentificare) şi în *record protocol* criptografia simetrică (ex.criptarea cu AES).**(2p)**

2. Vi se cere să faceţi un audit al unei aplicaţii web de comerţ electronic. Observaţi următoarele:

   - Credenţialele utilizatorilor se stochează în baza de date sub forma *(username, e-mail, H(password,salt))*, unde H este o funcţie hash proprietară. În caz de pierdere a parolei, aceasta se poate reseta prin accesarea unui link transmis pe e-mail. Valabilitatea acestui link este de 1 oră de la momentul generării, link-ul fiind generat folosind un PRNG cunoscut, care primeşte ca seed username-ul si ziua curentă.

- Conexiunea client-server este securizată prin TLS (la accesarea aplicaţiei web din browser puteţi vizualiza un certificat digital valid, emis de o autoritate recunoscută). Conform TLS, comunicarea client-server foloseşte două chei pentru asigurarea confidenţialităţii şi două pentru integritate, câte una pentru fiecare sens de comunicaţie.
- Stocarea locală a fişierelor confidenţiale (ex. a facturilor) se realizează direct în baza de date, după o criptare prealabilă AES-ECB.
- Integritatea end-to-end a mesajelor m transmise în modulul de chat (folosit pentru comunicarea cu reprezentanţii de vânzări) este asigurată de o funcţie $CRC(m)$, a cărei valoare se apendează mesajului transmis.
- Cu excepţia paginii de login, câmpurile de introducere date nu sunt sanitizate şi validate. Spre exemplu, aplicaţia permite introducerea unor date în trecut pentru ziua plasării comenzii, adaugarea unor preţuri negative, etc.

Răspundeţi la următoarele cerinţe:

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

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

(c) Ce puteţi spune despre confidenţialitatea, respectiv integritatea de la nivelul aplicaţiei? Argumentaţi. (1 paragraf) **(2x2.5p)**

(d) Daţi exemplu de un atac activ care vă poate permite logarea prin impersonarea unui alt utilizator. (1 paragraf) **(5p)**

3. Consideraţi varianta modificată de semnătură RSA (plecând de la standardul PKCS#1) definită astfel:

Fie $pk = (N, e)$ şi $sk = (p, q, d)$ cheile RSA publică, respectiv privată. Se semnează un mesaj m, $0 < |m| < |N|/2$, unde $|x|$ este dimensiunea în biţi a lui x astfel:

Pasul 1. Se realizează paddingul $m' = 0^8||0^71||FF^x||0^8||m$, unde $||$ este concatenare, 0^8 este un byte de 0, 0^71 este un byte cu primii 7 biţi 0 şi ultimul bit 1, FF^x este byte-ul FF repetat de x ori şi $x > 1$ este aleator ales astfel încât $0 \leq m' \leq N - 1$.

Pasul 2. Se obţine semnătura $\sigma = sign(m, sk) = m'^d \mod N$

(a) Explicaţi cum funcţionează funcţia de verificare a semnăturii $verif()$ în acest caz. Precizaţi în mod clar input-ul, output-ul şi modalitatea de calcul. **(5p)**

(b) Primiţi (m, σ) cu σ semnătură validă pentru m. Poate fi $(2m, 2^d\sigma)$ o semnătură validă? De ce/de ce nu? **(5p)**

(c) O extensie a acestei scheme permite semnarea mesajelor $|\bar{m}| \geq |N|/2$ prin adăugarea unui pas anterior:
Pasul 0. $\bar{m}$ se transformă în $0 < |m| < |N|/2$ astfel: $m = lsb_{|N|/2-1}(\bar{m} \mod N)$, unde lsb reprezină cei mai puţin semnificativi biţi.
Ilustraţi un atac asupra schemei astfel definită. **(5p)**

(d) Propuneţi o modificare simplă asupra schemei extinse pentru ca atacul anterior să nu mai funcţioneze. **(5p)**

4. Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ şi $T = \{0,1\}^{128}$. AND şi NOT sunt operaţiile logice cunoscute, pe biţi. Este MAC-ul de mai jos sigur? Argumentaţi. **(5p)**

   $Mac'(k,m) = Mac(k, m \text{ AND } NOT(m))$
   $Vrfy'(k,m,t) = Vrfy(k, m \text{ AND } NOT(m), t)$

TOTAL disponibile: 65p