

EXAMEN ONLINE - Instrucțiuni generale

1. Transmiteți examenul **prin Moodle** până la termenul limită: **27 ianuarie, ora 10:00**.
 - Transmiterea corectă a examenului este strict în responsabilitatea studenților.
 - Transmiteți în timp util, **NU** așteptați ultimele minute pentru a încărca examenul. Examenul poate fi transmis de oricâte ori doriți până la deadline, se ia în considerare doar ultima variantă transmisă. **NU** se acceptă ca motivație pentru netransmiterea examenului niciun fel de probleme tehnice (încetinirea platformei, utilizarea incorectă, nesincronizări ale ceasului platformei, etc.).
 - Studenții care nu transmit rezolvarea examenului scris sunt considerați absenți.
2. Răspunsul trebuie să fie în **format .pdf, încărcat prin contul instituțional Moodle** în secțiunea corespunzătoare sub numele **grupa_nume_prenume.pdf**. Prima pagină a fișierului de răspunsuri trebuie să conțină **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 (citeț / lizibil!), Word / LaTeX exportat în pdf, etc.
 - Aveți grijă ca fișierul final .pdf să fie valid și rezolvările să fie ușor identificabile!
3. Se acordă punctaje parțiale. Răspunsurile greșite la examenul scris **NU** depunțează suplimentar.
4. Pentru promovare, **este obligatoriu să participați la ambele probe (examen scris și oral), să obțineți minim 10 puncte la examenul final și minim 45 de puncte** ca notă finală (include punctele obținute în timpul anului).
5. Pentru examenul oral:
 - Este strict în responsabilitatea studenților să verificați repartizarea pe zile / ore (aprox.) și alte informații necesare referitoare la susținerea examenului oral.
 - Trebuie să vă conectați **audio-video, folosind contul instituțional Teams**.
 - Trebuie să arătați **un act de identitate**, de preferat **legitimăție / carnet de student cu poză**. Este în responsabilitatea studenților să ascundeți alte informații (altele decât numele și poza) de pe documentul prezentat, pe care nu doriți să le faceți publice!
 - Fiecare subiect rezolvat în scris, dar pe care nu știți să îl explicați (i.e., să arătați că l-ați rezolvat individual sau înțeles), **se depunțează cu dublul punctajului alocat subiectului respectiv**.
 - Studenții care transmit rezolvarea examenului scris dar nu participă la susținerea orală obțin nota finală 4.
 - Dacă există studenți care nu au posibilitatea unei conexiuni audio și video, trebuie să anunțe în prealabil, pe e-mail (*ruxandra.olimid@fmi.unibuc.ro*).

Dacă în timpul examenului aveți întrebări, le puteți posta pe forum, secțiunea *Examen*. Urmăriți forumul pentru informații. **NU postați indicii sau soluții!**

SUCCES!

EXAMEN ONLINE - Probleme**1. Adevărat sau Fals**

Răspundeți cu adevărat sau fals. Dacă afirmația este falsă, transformați-o într-o afirmație adevărată printr-o schimbare minimală (i.e., păstrați contextul, dar nu negați). Subliniați 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, ieșirea să conțină exact biții de intrare, permutați pseudoaleator (ex. pentru o cheie fixată K și $PRP_K : \{0, 1\}^4 \rightarrow \{0, 1\}^4$, $PRP_K(1101) = 1011$ 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 fișierelor în mod criptat. **(2p)**
 - (f) Pentru a asigura integritatea unor fișiere personale, este suficient să stocați pe calculatorul propriu fișierele și valoarea SHA256 corespunzătoare fiecăruia sub forma $(file1, SHA256(file1))$, $(file2, SHA256(file2))$ **(2p)**
 - (g) $SHA256(PAROLA) = 0x1c65fc11a8651621765d50083695b33b4de0d253ff984adb62f64e4c0504ed1f$. **(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 și q este întotdeauna mare. **(2p)**
 - (j) SSL/TLS implementează principiul diversității (*principle of diversity*) pentru că folosește în *handshake protocol* criptografia asimetrică (ex. certificate pentru autentificare) și în *record protocol* criptografia simetrică (ex. criptarea cu AES). **(2p)**
2. Vi se cere să faceți un audit al unei aplicații web de comerț electronic. Observați următoarele:
- Credențialele utilizatorilor se stochează în baza de date sub forma $(username, e-mail, H(password, salt))$, unde H este o funcție 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 primește ca seed username-ul și ziua curentă.

- Conexiunea client-server este securizată prin TLS (la accesarea aplicației web din browser puteți vizualiza un certificat digital valid, emis de o autoritate recunoscută). Conform TLS, comunicarea client-server folosește două chei pentru asigurarea confidențialității și două pentru integritate, câte una pentru fiecare sens de comunicație.
- Stocarea locală a fișierelor confidențiale (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 reprezentanții de vânzări) este asigurată de o funcție $CRC(m)$, a cărei valoare se appendează mesajului transmis.
- Cu excepția paginii de login, câmpurile de introducere date nu sunt sanitizate și validate. Spre exemplu, aplicația permite introducerea unor date în trecut pentru ziua plasării comenzii, adaugarea unor prețuri negative, etc.

Răspundeți la următoarele cerințe:

- Enunțați un principiu de securitate (referiți-vă la *Pages on Security - Principles*) care este satisfăcut. Argumentați. (1 paragraf) **(5p)**
 - Enunțați un principiu de securitate (referiți-vă la *Pages on Security - Principles*) care este NU este satisfăcut. Argumentați. (1 paragraf) **(5p)**
 - Ce puteți spune despre confidențialitatea, respectiv integritatea de la nivelul aplicației? Argumentați. (1 paragraf) **(2x2.5p)**
 - Dați exemplu de un atac activ care vă poate permite logarea prin impersonarea unui alt utilizator. (1 paragraf) **(5p)**
3. Considerați varianta modificată de semnătură RSA (plecând de la standardul PKCS#1) definită astfel:

Fie $pk = (N, e)$ și $sk = (p, q, d)$ cheile RSA publică, respectiv privată. Se semnează un mesaj m , $0 \leq m \leq (N - 1)/2$ astfel:

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

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

- Explicați cum funcționează funcția de verificare a semnăturii $\text{verif}()$ în acest caz. Precizați în mod clar input-ul, output-ul și modalitatea de calcul. **(5p)**
- Primiți (m, σ) cu σ semnătură validă pentru m . Poate fi $(2m, 2^d \sigma)$ o semnătură validă? De ce/de ce nu? **(5p)**
- O extensie a acestei scheme permite semnarea mesajelor $\bar{m} > N - 1$ prin adăugarea unui pas anterior:
Pasul 0. \bar{m} se transformă în $m \in [0, N - 1]$ astfel: $m = \bar{m} \mod N$.
 Ilustrați un atac asupra schemei astfel definită. **(5p)**
- Propuneți o modificare simplă asupra schemei extinse pentru ca atacul anterior să nu mai funcționeze. **(5p)**

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