Criptografie şi Securitate (ROL) - Restanţă: mai 2021

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **26 mai, ora 09:59**.
   - 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) şi să obţineţi minim 45 de puncte** ca notă finală (include punctele obţinute în timpul anului, fără bonus, care se acordă doar în caz de promovare).
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 - Refacerea / păstrarea punctajului

1. Pentru fiecare activitate, puteţi păstra punctajul deja obţinut sau reface punctajul aferent acesteia.

2. Menţionaţi clar activităţile pe care le refaceţi la începutul fişierului cu rezolvări pe care îl transmiteţi.

3. Dacă decideţi să refaceţi o activitate, **trebuie să transmiteţi rezolvările aferente** în acelaşi .pdf cu rezolvările examenului, la final. Excepţie fac problemele de seminar şi laborator, pe care le prezentaţi direct la examenul oral.

4. Activităţile din timpul anului pe care decideţi să le refaceţi vor fi prezentate la examenul oral.

5. Dacă decideţi să păstraţi punctajul din examenul scris, examenul transmis anterior va fi discutat la examenul oral.

6. Pentru refacerea activităţilor din timpul anului apar următoarele constrângeri:

   (a) NU se acceptă probleme de seminar şi laborator referitoare la sistemele clasice sau mecanice (Seminarul 1, Laboratoarele 1 şi 2).

   (b) Se acceptă doar blog-uri despre noţiuni / rezultate / sisteme / etc. din criptografia modernă (i.e., NU despre sisteme clasice, competiţii precum Cicada, etc.)

SUCCES!

EXAMEN ONLINE - Probleme

1. Sunt adevărate următoarele afirmaţii? Dacă da, precizaţi ADEVARAT, dacă nu, precizaţi FALS şi argumentaţi de ce afirmaţia nu este adevărată.

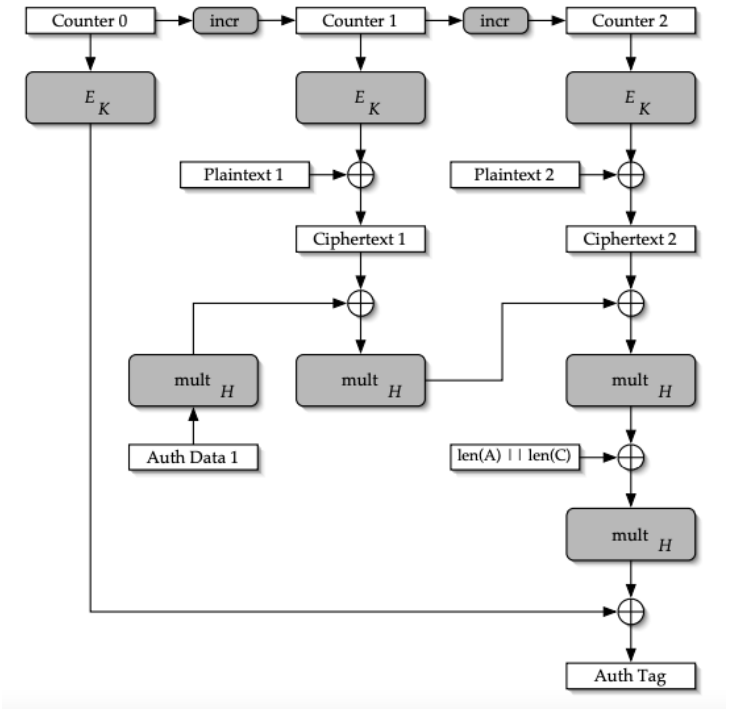
   (a) Sistemele de criptare se folosesc pentru a asigura confindenţialitatea datelor. **(2.5p)**

   (b) SHA-256 asigură integritatea datelor. **(2.5p)**

   (c) AES este standardul actual de criptare pentru sistemele fluide. **(2.5p)**

   (d) În cazul semnăturilor digitale, cheia privată se foloseşte pentru verificarea semnăturii. **(2.5p)**

2. Se consideră modul de operare GCM (Galois/Counter Mode), reprezentat în figura următoare pentru un mesaj clar (*plaintext*) de 2 blocuri (Plaintext 1, Plaintext 2):



Sursa imagine: McGrew, D. and Viega, J., 2004. The Galois/counter mode of operation (GCM). Submission to NIST Modes of Operation Process, 20, pp.0278-0070

Bineînţeles, generalizând, modul de operare poate fi utilizat pentru criptarea unui mesaj de lungime oarecare. Pentru simplificare, considerăm *Counter 0* o valoare aleatoare, aleasă la fiecare criptare şi transmisă către destinaţie ca prima componentă a mesajului criptat (*ciphertext*).

(a) Ce reprezintă notaţia E_k? **(2.5p)**

(b) Menţionaţi dacă E_k trebuie să fie inversabil. Argumentaţi. **(2.5p)**

(c) Daţi un exemplu de sistem cunoscut care poate fi utilizat ca E_k. **(2.5p)**

(d) Interceptaţi mesajul criptat (Cipertext 1, Ciphertext 2) cu o lungime totală de 192 biţi (fără să consideraţi şi dimensiunea lui *Counter 0*). Ce puteţi spune despre lungimea mesajului clar? **(2.5p)**

(e) Câte valori poate lua *Counter 0* dacă este reprezentat pe 128 biţi? Ce puteţi spune despre securitatea sistemului în acest caz? **(2x2.5p)**

(f) Oscar interceptează *Counter 0* şi (Cipertext 1, Ciphertext 2). Cum ar putea proceda Oscar ca să determine mesajul clar corespunzător dacă are acess la un oracol de criptare E_k (i.e., un oracol care primind ca input x întoarce $E_k(x)$, cu x de dimensiunea unui bloc)? **(2.5p)**

3. Se consideră sistemul de criptare Textbook RSA pentru care $N = 1189$.

(a) Poate fi $e = 122$ un coeficient de criptare valid? Argumentaţi. **(2.5p)**

(b) Fie $e = 121$. Care este criptarea lui 1? Dar a lui 1188? **(2x2.5p)**

(c) $m_1 = 11$ se criptează în 872 şi $m_2 = 171$ se criptează în 704. Care este criptarea lui $m = 11 \cdot 171$? **(2.5p)**

(d) Cât este lungimea recomandată în biţi a modulului RSA la momentul actual? **(2.5p)**

(e) Este Texbook RSA CPA-sigur? Argumentaţi folosind definiţia securităţii CPA. **(2.5p)**

4. Vi se cere părerea în realizarea unui audit intern la locul de muncă.

Observaţi că se utilizează *CryptStream*, un sistem de criptare de tip fluid care foloseşte ca generator $G(x) = x||2x$, unde x este seed-ul de intrare şi $||$ este concatenare, pentru comunicaţia criptată cu clienţii. x se obţine ca un derivat din parola *pwd* asociată clientului: $x = F(SHA256(pwd, salt))$, cu F funcţie *one-way* (deterministă) cunoscută.

(a) Este G din *CryptStream* PRG (sigur din punct de vedere criptografic)? Argumentaţi. **(2.5p)**

(b) Care este mesajul clar m corespunzător unui mesaj criptat c transmis unui client (se presupune x cunoscut) folosind *CryptStream*? Scrieţi formula de decriptare. **(2.5p)**

(c) Observaţi o eroare de implementare din cauza căreia valoarea *salt* este mereu constantă, egală cu 0. Ce puteţi spune în acest caz? **(2.5p)**

(d) Găsiţi în documente definiţia a două funcţii f şi h. $f : \{0,1\}^m \to \{0,1\}^m$ o funcţie bijectivă rezistentă la prima preimagine. Pentru orice $x \in \{0,1\}^{2m}$ se defineşte $h : \{0,1\}^{2m} \to \{0,1\}^m$ astfel: $h(x) = f(x') \oplus x''$, unde $x = x'||x''$ şi $x', x'' \in \{0,1\}^m$. Realizaţi că h nu este rezistentă la a doua preimagine. Argumentaţi. **(5p)**

(e) Protocolul *Diffie-Hellman* este folosit în cadrul companiei, implementat peste un grup pentru care un adversar PPT poate rezolva *Problema Logaritmului Discret* (PLD, sau DLP în limba engleză) cu o probabilitate constantă $f(n) = 10^{-8}$, indiferent de valoarea parametrului de securitate n. Ce puteţi spune despre securitatea protocolului de schimb de chei *Diffie-Hellman* în acest caz? **(2.5p)**

(f) Observaţi de asemenea că protocolul *Diffie-Hellman* este vulnerabil la un atac de tip Man-in-the-Middle. Propuneţi o soluţie. **(2.5p)**

5. **(Optional)** Formular anonim de feedback: `https://forms.gle/DhBHMKadQo8SZCzSA`. Acest formular NU înlocuieşte formularul de feedback oficial primit prin facultate, pe care vă încurajez să îl completaţi la momentul respectiv.

TOTAL disponibile: 60p