Criptografie şi Securitate (ROL) - Examen: mai 2021

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **19 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 - Probleme

1. Există o tendinţă de a face confuzie între criptare şi aplicarea unei funcţii hash.

   (a) Explicaţi pe scurt câte un scenariu potrivit pentru fiecare dintre cele 2 situaţii (e.g., un exemplu de aplicaţie când această abordare este potrivită, etc.) şi motivaţi de ce aţi făcut această alegere (2 paragrafe, câte unul pentru fiecare subpunct):

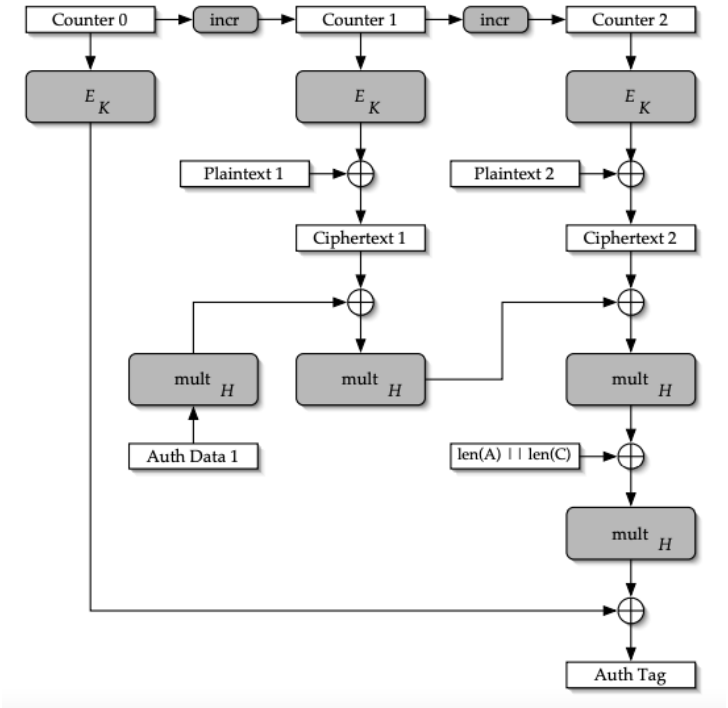
      (i) stocarea parolelor se realizează folosind o funţie hash (i.e., parolele sunt "hash-uite") **(2.5p)**

      (ii) stocarea parolelor se realiează folosind o funcţie de criptare (i.e., parolele sunt criptate) **(2.5p)**

   (b) Enuntaţi un aspect care diferenţiază clar un sistem de criptare de o funcţie hash. **(2.5p)**

   (c) Explicaţi pe scurt (1 paragraf) de ce nu putem considera securitate perfectă (ci doar computaţională) în cazul funcţiilor hash. **(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) Scrieţi formula de criptare. **(2.5p)**

(b) Scrieţi formula de decriptare. **(2.5p)**

(c) Consideraţi că E_K este o funcţie de criptare bloc cu lungimea blocului de 128 biţi. Mesajul clar are lungimea 320 biţi. Care este lungimea în biţi a mesajului criptat, fără să consideraţi şi dimensiunea lui *Counter 0* (i.e., consideraţi doar (Cipertext 1, Ciphertext 2, ...)? Consideraţi soluţia cea mai eficientă. **(2.5p)**

(d) Considerăm în acelaşi context de la întrebarea precedentă şi tag-ul de autentificare *Auth Tag*. Câţi biţi se adaugă mesajului criptat (i.e., care este lungimea tag-ului)? **(2.5p)**

(e) Explicaţi pe scurt (1 paragraf) ce aduce GCM în plus faţă de modul de operare CTR din punct de vedere al securităţii. **(2.5p)**

(f) Este adevărată următoarea afirmaţie: *"Pentru că lungimea blocului este mare (egală cu* 128 *biţi), rezultă că sistemul definit mai sus este perfect sigur."*? Argumentaţi. **(2.5p)**

3. Se consideră cheia publică RSA stocată în fişierul *RSA_public_key.txt* (disponibil în Moodle, secţiunea *Examen*).

(a) Folosiţi un ASN.1 decoder (disponibil online) pentru a determina valoarea modulului N şi a exponentului e. Scrieţi valoarea lui e şi dimensiunea în biţi ai lui N. **(2.5p)**

(b) Consideraţi că un alt user deţine o cheie publică RSA pentru care $e = 65537$. Ce puteţi spune despre N? Argumentaţi. **(2.5p)**

(c) Se consideră următoarea variantă a RSA Padded. Fie $|m| \approx |N|/2$ (mesaje de aproximativ jumătate din lungimea modulului în biţi). Definim $\bar{m} = 0^8||r||m$, unde 0^8 este un byte cu toţi biţii egali cu 0, r este ales uniform aleator (pe numărul de biţi rămaşi) şi $||$ este concatenare. Atunci $c = \bar{m}^e \mod N$. Arătaţi că sistemul astfel definit nu este CCA-sigur. **(5p)**

(d) Funcţionează atacul de la punctul precedent şi pentru PKCS#1 v1.5, definit în curs? Argumentaţi. **(2.5p)**

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

(a) O aplicaţie de comunicare externă foloseşte funcţia hash SHA-256 pentru asigurarea integrităţii datelor. Cum vi se pare această abordare? Argumentaţi. **(2.5p)**

(b) 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)**

(c) Observaţi că h definită la punctul anterior este folosită pentru calculul amprentei fişierelor înainte de a fi semnate. Mai exact, pentru un fişier cu reprezentarea binară x se calculează $h(x)$ care apoi se semnează folosind o semnătură digitală. Puteţi evidenţia cel puţin o problemă? **(2.5p)**

(d) Propuneţi o soluţie ca să rezolvaţi problema pe care aţi evidenţiat-o la punctul anterior. **(2.5p)**

(e) Pentru asigurarea confidenţialităţii observaţi că se foloseşte un sistem de criptare fluid pentru care cheia fluidă este $k = G(day)$, unde G este un PRG (generator de numere pseudo-aleatoare sigur din punct de vedere criptografic), iar *day* este ziua curentă, sub forma *yyyymmdd*. Cum vi se pare această abordare? Argumentaţi. **(2.5p)**

(f) Vi se refuză accesul la implementarea schemei $(Mac, Vrfy)$, utilizată la nivel managerial, pe motiv că aceasta este proprietară şi secretă. Ce principiu al criptografiei este încălcat? **(2.5p)**

5. Considerăm următorul protocol de schimb de chei:

(1) Alice alege uniform aleator $k, a \leftarrow \{0,1\}^n$ şi îi trimite lui Bob $s = k \oplus a$;

(2) Bob alege uniform aleator $b \leftarrow \{0,1\}^n$ şi îi trimite lui Alice $u = s \oplus b$;

(3) Alice calculează $w = u \oplus a$ şi îi trimite w lui Bob;

(4) Alice consideră drept cheie comună k iar Bob calculează drept cheie comună $w \oplus b$.

(a) Arătaţi că Bob calculează aceeaşi cheie k. **(2.5p)**

(b) Este schema astfel definită sigură faţă de un adversar pasiv? Dacă da, de ce? Dacă nu, explicaţi pe scurt un atac concret. **(5p)**

(c) Propuneţi o modalitate sigură în care Alice şi Bob pot stabili o cheie comună chiar şi în cazul unui adversar activ. **(2.5p)**

6. **(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: 65p