Criptografie şi Securitate (ROL) - Examen: mai 2020

EXAMEN ONLINE - Instrucţiuni generale

1. Transmiteţi examenul **prin Moodle** până la termenul limită: **21 mai, ora 09:55**.
   - Transmiterea corectă a examenului este strict în responsabilitatea voastră.
   - 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, 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 voastră 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** (CI, paşaport, permis de conducere, etc.) **sau legitimaţie de student cu poză**. Este în responsabilitatea voastră 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, secţiunile *Examen* sau *Întrebări exerciţii şi probleme examen*. Urmăriţi formul pentru informaţii. **NU postaţi indicii sau soluţii!**

SUCCES!

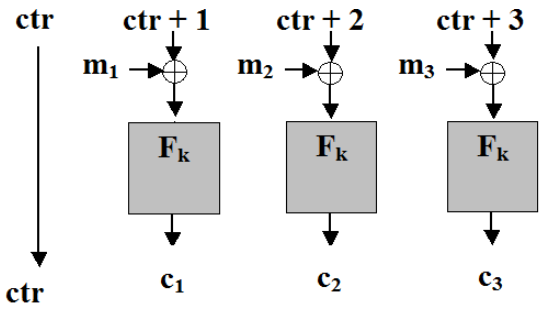
EXAMEN ONLINE - Probleme

1. Primiţi de la Alice următorul mesaj criptat: $C = 45A4562AB1C307F78ED2$ (în reprezentare hexa). Ştiţi că mesajul este criptat cu One Time Pad (OTP) cu o cheie K stocată pe un stick, pe care din neglijenţă l-aţi pierdut.

   (a) Ce puteţi spune despre cheia K stocată pe stick dacă ştiţi că sistemul vă permitea comunicarea perfect sigură? **(2.5p)**

   (b) Alice află că aţi pierdut cheia. Vă transmite un alt mesaj criptat C', corespunzător aceluiaşi mesaj clar M. Vă anunţă (public) că pentru criptare a folosit o cheie $K = M$ (i.e., C' este criptarea mesajului M folosind cheia $K = M$). Sistemul de criptare folosit rămâne OTP. Ce puteţi afirma despre C' în această situaţie? Puteţi decripta? **(2.5p)**

2. Se consideră modul de operare CTR_{modif} (Counter Mode Modificat), reprezentat în figura de mai jos pentru un mesaj clar $m = (m_1, m_2, m_3)$ de 3 blocuri:



   Bineînţeles, generalizând, modul de operare poate fi utilizat pentru criptarea unui mesaj de lungime oarecare. Notaţiile trebuie să vă fie cunoscute de la modul de operare CTR. *ctr* este o valoare aleasă uniform aleator pentru fiecare mesaj.

   (a) Care este mesajul criptat? Scrieţi formula de criptare. **(2.5p)**

   (b) Desenaţi schema de decriptare. Scrieţi formula de decriptare. **(2x2.5p)**

   (c) Se foloseşte padding-ul *0-peste-tot*, adică se adaugă 0 pentru completarea ultimului bloc. Dacă mesajul m este multiplu de lungimea blocului, nu se mai realizează padding-ul. Ce puteţi spune despre corectitudinea sistemului? Dar dacă s-ar realiza padding-ul indiferent de situaţie (i.e., dacă mesajul m este multiplu de lungimea blocului, se adaugă un bloc *0-peste-tot*)? **(2x2.5p)**

   (d) Este sistemul de criptare CCA sigur? Argumentaţi.**(5p)**

   (e) Se consideră lungimea blocului egală cu 48 de biţi (6 bytes). Ce puteţi afirma în plus despre securitatea sistemului în acest caz? **(2.5p)**

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

   - $MD5$, funcţie hash folosită pentru stocarea parolelor clienţilor cu *salt*.
   - $CryptStream$, un sistem de criptare de tip fluid care foloseşte ca generator $G(x) = x^2 \pmod{x}$, unde x este seed-ul de intrare, pentru comunicaţia criptată cu clienţii. x se obţine ca un derivat din parola pwd asociată clientului: $x = F(MD5(pwd, salt))$, cu F funcţie *one-way* (deterministă) cunoscută.
   - Protocolul de schimb de chei *Diffie-Hellman* neautentificat pentru generarea cheilor necesare securizării comunicaţiei interne (i.e., între angajaţii firmei) într-un grup pentru care un adversar PPT poate rezolva *Problema Logaritmului Discret* (PLD, sau DLP în limba engleză) cu o probabilitate $f(n) = 1/n^{65537}$, cu n parametrul de securitate.
   - $AuthMAC$, un sistem de autentificare proprietar utilizat pentru autentificarea părţilor în comunicaţia dintre manageri. În urma semnării unui *Non Disclosure Agreement (NDA)*, vi s-a dat acces la descrierea acestuia:
     $Mac(k, m) = h(k||len(m)) \oplus h(m)$, unde h este o funcţie hash rezistentă la coliziuni, $||$ este concatenare, $len(m)$ este lungimea în biţi a mesajului m, $\oplus$ este operatorul pe biţi XOR.
     $Vrfy(k, m, t) = \begin{cases} 1 & \text{dacă } Mac(k, m) = t \\ 0, & \text{altfel} \end{cases}$

   Vi se cere să completaţi un raport care să răspundă la următoarele întrebări:

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

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

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

   (d) Ce puteţi spune despre funcţia f şi securitatea protocolului de schimb de chei *Diffie-Hellman* în acest caz? **(2.5p)**

   (e) Presupunând că se setează nişte parametrii pentru care *problema decizională Diffie-Hellman (DDH)* este dificilă, la ce tip de atac rămâne vulnerabil protocolul de schimb de chei? Cum s-ar putea împedica un astfel de atac? **(2x2.5p)**

   (f) Este $AuthMAC$ un sistem de autentificare a părţilor sigur (din punct de vedere criptografic)? Argumentaţi. **(5p)**

   (g) Există principii cunoscute în criptografie care sunt încălcate? Dacă da, daţi un exemplu, specificând numele principiului şi cum / de ce este încălcat. **(2.5p)**

   (h) Ce obiective ale criptografiei ar trebui să fie satisfăcute în mod normal într-un astfel de scenariu (comunicaţia internă şi externă a unei companii), dar în condiţiile date sunt încălcate? Daţi 2 exemple. **(2x2.5p)**

4. Se consideră sistemul de criptare RSA pentru care valoarea modulului N este (în reprezentare hexa):

   N = 22 A1 E6 5B 83 51 5A 43 47 BC 69 14 A3 00 13 7C 8E D0 80 43 00 8D 0C D5 E1 FE 44 4F DB A3 5E C4 1C B4 15 85 12 BB B2 AD DA FD FA 32 EE B4 38 A2 20 4E DD 64 D6 BC 78 7E 4B 42 CC 37 09 77 C6 23 F4 46 96 61 8D D6 CA E9 5D 71 E2 97 84 1E BD 85 6D 39 21 C1 A5 92 FD 5B E7 37 32 C3 1C 04 33 69 2E 58 4F A4 D0 1D D5 BC 95 28 ED AC 03 74 AD 55 5D 7B 92 79 26 0A 51 5B 5A 20 9C 86 3C 14 91 9A C7 58 21 80 59 A5 EA 50 C2 A9 07 3A 67 CD 9D 99 CB E2 57 C3 45 EB 3C C9 2B 55 04 9E 8D FD 92 26 35 6D 5C 41 F6 61 4B 0B 2D 96 92 AF 92 8B 00 38 49 3F C2 EC F7 A8 F1 A9 24 43 98 7B 7D 22 87 31 82 27 DF 9F DA 27 85 EB 85 48 E2 D2 61 3F 09 0F 9B C7 31 56 8B C0 08 38 05 D6 DE 76 75 E2 3D A1 33 BC C2 90 05 F8 3C DD FC 80 B0 BE 3E AB 45 22 46 1D 35 1D 0F 6E 34 EA 8F A0 27 42 48 6A 8C D8

   (a) Exponentul de criptare este $e = 65537$. Este sistemul corect definit dacă foloseşte aceşti parametrii? Argumentaţi. **(2.5p)**

   Se decide înlocuirea RSA cu un sistem de criptare definit peste curba eliptică $y^2 = x^3 + 17x + 3 \pmod{29}$.

   (b) Care este inversul punctului $(8, 10)$? Dar al punctului (8,11)? **(2x2.5p)**

   (c) Ce puteţi spune despre curba eliptică dată din punct de vedere al securităţii? **(2.5p)**

   (d) Căutaţi un exemplu de curbă eliptică de această formă recomandată de o instituţie cunoscută (NIST, ENISA, etc.). Specificaţi numele exact sub care este cunoscută curba şi ecuaţia acesteia (specificând şi modulul p). **(2.5p)**

5. Completaţi următorul formular (accesibil şi după deadline):

   `https://forms.gle/YfpsXsawvqMMN1bT8` **(0p)**

TOTAL disponibile: 65p