Criptografie si Securitate EXAMEN Timp de lucru: 2h

Nume: _____ Grupă: _____

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 corect: Fals. RSA este un sistem de criptare ***asimetric****.*

   (a) Sistemul OTP sigur permite folosirea unei singure chei de criptare pentru mai multe mesaje diferite atâta timp cât lungimea cheii este cel puţin la fel de mare ca lungimea mesajelor. **(2p)**

   (b) Este recomandat să se folosească AES pentru transmiterea fişierelor de dimensiuni mari. **(2p)**

   (c) Pentru schimbul de chei Diffie-Hellman este esenţial ca cele două părţi să partajeze în avans un secret. **(2p)**

   (d) Pentru a asigura integritatea mesajelor, este suficient să le trimitem criptate cu un sistem de criptare public şi sigur. **(2p)**

   (e) La crearea semnăturilor digitale, are mai mult sens mai întâi să semnăm mesajul şi apoi să îl comprimăm cu o funcţie hash.

   (f) Timpul necesar unui atacator pentru a găsi coliziuni pentru funcţia hash SHA-256 este de 2^{256}. **(2p)**

   (g) Nerepudierea îi permite lui Bob să prezinte spre verificare unei terţe părţi un document semnat de Alice şi această proprietate este asigurată numai de codurile de autentificare a mesajelor (MAC). **(2p)**

   (h) Combinaţia autentifică-apoi-criptează este întotdeauna sigură indiferent de cum sunt instanţiate componentele ei. **(2p)**

   (i) Sistemele de criptare post-cuantice sunt sisteme de criptare care folosesc metode cuantice pentru asigurarea securităţii în faţa unui adversar clasic. **(2p)**

   (j) Protocolul TLS este folosit de către browser-ul web de fiecare dată când realizează o conexiune sigură cu un site web folosind *http*. **(2p)**

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

   - Sistemul de criptare AES pentru stocarea criptată a fişierelor unde cheia pentru criptare/decriptare este generata cu un PRNG cunoscut care primeste ca seed ziua si numele companiei.
   - Funcţia hash SHA-2 pentru stocarea parolelor clienţilor (de 6 caractere) cu un *salt* pe 8 biţi.
   - Protocolul de schimb de chei Diffie-Hellman autentificat (deci rezistent la un atac de tip man-in-the-middle) pentru generarea cheilor necesare securizării comunicaţiei interne (i.e., între angajaţii firmei) într-un grup $\mathbb{G}$ în care problema logaritmului discret este uşoară. O cheie astfel generată este apoi utilizată ca şi cheie secretă a sistemului de criptare 3DES pentru transmiterea criptată a mesajelor.

- Site-ul web al companiei este securizat folosind certificate digitale cu modulul RSA N pe 128 biţi.
- Integritatea end-to-end a mesajelor m transmise în modulul de chat (folosit pentru comunicarea în cadrul companiei) este asigurată de algoritmul simetric de criptare DES aplicat mesajului, a cărui valoare se apendează mesajului transmis.

Răspundeţi la următoarele cerinţe:

(a) Sunt parolele clienţilor stocate în mod sigur? Dar fişierele criptate? Argumentaţi. (1 paragraf) **(10p)**

(b) Ce puteţi spune despre securitatea sistemului RSA folosit în cadrul certificatelor digitale? Argumentaţi(1 paragraf) **(5p)**

(c) Există alte probleme de securitate (confidenţialitate, integritate) la nivelul aplicaţiei? Argumentaţi. (1 paragraf) **(5p)**

3. Se consideră modul de operare definit mai jos pentru criptarea unei secvenţe de blocuri de text clar $m_1||m_2||m_3||\ldots$ într-o secvenţă de blocuri $c_1||c_2||c_3||\ldots$:

$$c_i = F_{k_2}(c_{i-1} \oplus F_{k_1}(m_{i-1} \oplus m_i)), i \geq 1$$

unde m_0 şi c_0 sunt vectori de iniţializare publici şi fixaţi.

(a) Ce reprezintă notaţia F_{k_i}, pentru $i \in \{1, 2\}$? Ce proprietate esenţială trebuie să satisfacă funcţia F_{k_i} pentru ca sistemul să fie corect?**(2 × 2.5p)**

(b) Indicaţi cum se realizează decriptarea. **(7.5p)**

(c) Câte valori posibile pot lua m_0 şi c_0 dacă sunt reprezentate fiecare pe 16 biţi? **(2.5p)**

(d) Presupunând că un bloc c_i suferă erori de transmisie, care blocuri de text clar sunt impactate? **(5p)**

4. Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ şi $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentaţi răspunsul.

$Mac'(k, (m_1, m_2)) = Mac(k, m_1 \oplus m_2)$

$Vrfy'(k, (m_1, m_2), t) = Vrfy(k, (m_1, m_2), t)$

(5p)