Securitatea Sistemelor Informatice - Sesiunea: mai 2025

EXAMEN

NUME: ..... GRUPA: .....

Timp efectiv de lucru: 1h 45 min. TOTAL: 65p

Notă: Pentru promovare, **este obligatoriu să obţineţi min.10p la examenul final şi min.45p** ca notă finală (include punctele obţinute în timpul anului).

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).

   Exemplu: RSA este un sistem de criptare simetric.
   Răspuns: Fals. RSA este un sistem de criptare ~~simetric~~ asimetric.

   (a) Modul de operare ECB este nedeterminist. **(2p)**

   (b) La criptarea mesajelor cu OTP, cheia nu trebuie refolosită. **(2p)**

   (c) În criptografia asimetrică, cheia privată se foloseşte pentru criptare. **(2p)**

   (d) SHA3 este o funcţie hash considerată sigură. **(2p)**

   (e) Criptarea asimetrică este în general mai eficientă decât criptarea simetrică. **(2p)**

   (f) Funcţiile hash au ca scop protejarea modificării conţinutului unui mesaj, deci protejarea integrităţii mesajului împotriva unor adversari maliţioşi. **(2p)**

   (g) În contextul unui adversar, PPT se referă la Probabilistic Polynomial Time. **(2p)**

   (h) AES este un sistem de criptare fluid. **(2p)**

   (i) O valoare de tip *nonce* este prin definiţie secretă. **(2p)**

   (j) Un atac de tip Meet-in-the-Middle se realizează asupra unei criptări DES simple (unice) .**(2p)**

2. Fie E un sistem de criptare simetric de tip bloc cu lungimea blocului de 64 biţi. Cheile de criptare sunt, de asemenea, secvenţe binare pe 64 biţi. Sistemul se foloseşte în modul de operare CTR, cu menţiunea că valoarea counter-ului porneşte de la 0 ($ctr_0 = 0$) şi ia numai valori pare, i.e., creşte mereu cu 2 ($ctr_i = ctr_{i-1} + 2$, $i > 0$).

   (a) Considerând cheile alese uniform aleator din spaţiul cheilor, câte chei posibile există? **(5p)** .....

   (b) Care este lungimea, în biţi a valorii counter? **(5p)** .....

   (c) Scrieţi formula de criptare pentru E in CTR mode astfel definit. **(5p)** .....
   .....

   (d) Cum influenţează incrementarea counter-ului cu 2 (în loc de 1) securitatea criptării? **(5p)** .....

3. Se consideră modalitatea de padding *OAEP* modificată definită ca $OAEP(m,r) = x_1 \| x_2$ unde

$$x_1 = H(r) \oplus 1^{n/2} \| m$$
$$x_2 = G(x_1) \oplus r$$

unde $m \in \{0,1\}^{n/2}$, r este o valoare aleatoare pe n biți, G și H sunt 2 funcții hash pe n biți.

(a) Care este lungimea în biți a $OAEP(m,r)$? **(2.5p)** .....

(b) Se poate defini o schemă de padding sigură pentru RSA dacă output-ul este de aceeași lungime cu input-ul? Argumentați. **(5p)** .....
.....

(c) Determinați $OAEP^{-1}$, i.e. cunoscând $OAEP(m,r) = x_1 \| x_2$, indicați cum se calculează m. **(2.5p)** .....
.....

4. Sunteți angajat să verificați securitatea în cadrul unei companii unde se folosesc:

- *Protocolul de schimb de chei Diffie-Hellman* autentificat pentru generarea cheilor necesare securizării comunicației interne (i.e., între angajații firmei) într-un grup pentru care un adversar PPT poate rezolva *Problema Logaritmului Discret* (PLD, sau DLP în limba engleză) cu o probabilitate constantă $f(n) = 10^{-5}$, indiferent de valoarea parametrului de securitate n. Autentificarea se realizează folosind certificate digitale cu modulul RSA N pe 512 de biți.
- *AuthMAC*, un sistem de autentificare utilizat pentru autentificarea entităților comunicante: $Mac(k,m) = H(m_s \| k) \| H(m_d \| k)$, unde H este o funcție hash rezistentă la coliziuni, $\|$ este concatenare, m_s și m_d jumătatea stângă, respectiv dreaptă a lui m (pentru m de lungime impară se consideră m_s mai lung cu 1 bit decât m_d).

$$Vrfy(k,m,t) = \begin{cases} 1 & \text{dacă } Mac(k,m) = t \\ 0, & \text{altfel} \end{cases}$$

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

(a) Ce puteți spune despre funcția f și securitatea protocolului de schimb de chei *Diffie-Hellman* în acest caz? **(2.5p)** .....
.....

(b) Ce puteți spune despre securitatea sistemului RSA folosit în cadrul certificatelor digitale? Puteți propune o îmbunătățire? **(2x2.5p)** .....
.....
.....

(c) Puteți afirma ceva despre confidențialitatea datelor? **(2.5p)** .....
.....

(d) Este *AuthMAC* un sistem de autentificare sigur? Argumentați. **(5p)** .....