Securitatea Sistemelor Informatice - Examen (A)

Sesiunea: februarie 2024
Timp efectiv de lucru: 1h 45min

1. (1p = 5 x 0,2p) Explicați fiecare din termenii:
   (a) Confidențialitate
   (b) Dropper
   (c) Troian
   (d) Inginerie socială
   (e) One-way function
2. (1p = 4 x 0,25p) Răspundeți cu adevărat sau fals pentru fiecare dintre următoarele afirmații. Argumentați pe scurt fiecare răspuns.
   (a) Este corect să stocăm o parolă în formă criptată?
   (b) Este corect să utilizăm modul ECB pentru criptarea datelor?
   (c) Este corect să reutilizăm cheia la criptarea mesajelor cu OTP?
   (d) Există funcții hash fară coliziuni?
3. (1p) Sistemul de criptare RSA.
   (a) (0,2p) Descrieți criptosistemul RSA.
   (b) (0,4p) Fie $n = 2911 = 41 \cdot 71$. Care dintre cele trei valori reprezintă o cheie de criptare validă: $3, 5, 8$? Argumentați.
   (c) (0,4p) Fie $e = 11$. Care dintre cele trei valori reprezintă cheia de decriptare corespunzătoare: $2289, 2291, 2294$? Argumentați.
4. (1p = 2 x 0,5p) Fie sistemul de criptare afin, definit astfel: $c \equiv a \cdot m + b \bmod 29$, unde m este mesajul pe care dorim să îl criptăm.
   (a) Ce valori posibile poate lua a?
   (b) Calculați a și b știind perechiile $(m, c) \in \{(10, 24), (12, 5)\}$.
5. (1p = 2 x 0,5p) Prezentați sistemul de criptare ElGamal. Definiți o problemă dificilă pe care se bazează acesta.
6. (1p = 2 x 0,5p) Prezentați atacul de tip Man-in-the-Middle. Exemplificați un scenariu de atac, indicând cum/în ce condiții se poate realiza un astfel de atac.
7. (1p - bonus) Pentru un mesaj m se calculează criptarea c folosind un sistem de criptare CCA-sigur și tag-ul t folosind un Message Authentication Code (MAC) sigur. Se transmite pe un canal de comunicație nesecurizat perechea (c, t). Ce puteți spune despre confidențialitatea mesajului m? Discuție.

Securitatea Sistemelor Informatice - Examen (B)

Sesiunea: februarie 2024
Timp efectiv de lucru: 1h 45min

1. (1p = 5 x 0,2p) Explicați fiecare din termenii:
   (a) Integritate
   (b) Downloader
   (c) Malware
   (d) Phishing
   (e) Funcție rezistentă la coliziuni
2. (1p = 4 x 0,25p) Răspundeți cu adevărat sau fals pentru fiecare dintre următoarele afirmații. Argumentați pe scurt fiecare răspuns.
   (a) Este corect să criptăm mesaje cu o cheie harcodată în cod?
   (b) Este corect să utilizăm DES pentru criptarea datelor?
   (c) Este corect să refolosim aceeași valoare aleatoare la criptarea datelor cu ElGamal?
   (d) Există funcții hash fară coliziuni?
3. Sistemul de criptare RSA.
   (a) (0,2p) Descrieți criptosistemul RSA.
   (b) (0,4p) Fie $n = 2881 = 43 \cdot 67$. Care dintre cele trei valori reprezintă o cheie de cifrare validă: $3, 5, 10$? Argumentați.
   (c) (0,4p) Fie $e = 13$. Care dintre cele trei valori reprezintă cheia de decriptare corespunzătoare: $851, 853, 856$? Argumentați.
4. (1p = 2 x 0,5p) Fie sistemul de criptare afin, definit astfel: $c \equiv a \cdot m + b \bmod 31$, unde m este mesajul pe care dorim să îl criptăm.
   (a) Ce valori posibile poate lua a?
   (b) Calculați a și b știind perechiile $(m, c) \in \{(10, 22), (12, 3)\}$.
5. (1p = 2 x 0,5p) Prezentați sistemul de criptare ElGamal. Definiți o problemă dificilă pe care se bazează acesta.
6. (1p = 2 x 0,5p) Prezentați atacul de tip Man-in-the-Middle. Exemplificați un scenariu de atac, indicând cum/în ce condiții se poate realiza un astfel de atac.
7. (1p - bonus) Pentru un mesaj m se calculează criptarea c folosind un sistem de criptare CCA-sigur și tag-ul t folosind un Message Authentication Code (MAC) sigur. Se transmite pe un canal de comunicație nesecurizat perechea (c, t). Ce puteți spune despre confidențialitatea mesajului m? Discuție.

Securitatea Sistemelor Informatice - Examen (C)

Sesiunea: februarie 2024
Timp efectiv de lucru: 1h 45min

1. (1p = 5 x 0,2p) Explicați fiecare din termenii:
   (a) Disponibilitate
   (b) Riskware
   (c) Computer worm (vierme)
   (d) Spear phishing
   (e) Modul de operare CTR (schema)

2. (1p = 4 x 0,25p) Răspundeți cu adevărat sau fals pentru fiecare dintre următoarele intrebari/afirmații. Argumentați pe scurt fiecare răspuns.
   (a) Este corect să utilizăm un salt harcodat în cod, aceelasi pentru stocarea tuturor parolelor?
   (b) Este corect să utilizăm cheia privată pentru criptarea mesajelor?
   (c) Este corect să utilizăm SHA512 ca funcție hash?
   (d) In cazul cel mai nefavorabil, un atac de tip brute force pentru o cheie de 256 biți necesită 2^{256} încercări.

3. Sistemul de criptare ElGamal.
   (a) (0,2p) Descrieți criptosistemul ElGamal.
   (b) (0,4p) Fie $g = 2$ un generator pentru $\mathbb{Z}_{29}^*$. Pentru cheia secretă $x = 11$, care dintre cele trei valori reprezintă o cheie publică validă $h : 7, 11, 18$? Argumentați.
   (c) (0,4p) Criptaţi un mesaj $m \in \mathbb{Z}_{29}^*$ la alegere.

4. (1p = 2 x 0,5p) Răspundeți la următoarele cerințe.
   (a) Două dintre cele trei module RSA $576077, 571367, 568507$ au un factor comun. Care este acesta?
   (b) Calculați simbolul Legendre al lui 7 modulo factorul comun.

5. (1p = 2 x 0,5p) Prezentați protocolul de schimb de chei Diffie-Hellman. Definiți o problemă dificilă pe care se bazează acesta.

6. (1p = 2 x 0,5p) Prezentați atacul de tip Meet-in-the-Middle. Exemplificați un scenariu de atac, indicând cum/în ce condiții se poate realiza un astfel de atac.

7. (1p - bonus) Pentru un mesaj m se calculează criptarea c folosind un sistem de criptare CCA-sigur și tag-ul $t = H(m)$, unde H este o funcție hash rezistenta la coliziuni. Se transmite pe un canal de comunicație nesecurizat perechea (c, t). Ce puteți spune despre integritatea mesajului m? Discuție.

Securitatea Sistemelor Informatice - Examen (D)

Sesiunea: februarie 2024
Timp efectiv de lucru: 1h 45min

1. (1p = 5 x 0,2p) Explicați fiecare din termenii:
   (a) Non-repudiere
   (b) Ransomware
   (c) Virus
   (d) Whaling
   (e) Modul de operare CBC (schema)
2. (1p = 4 x 0,25p) Răspundeți cu adevărat sau fals pentru fiecare dintre următoarele intrebari/afirmații. Argumentați pe scurt fiecare răspuns.
   (a) Este corect să utilizăm parole harcodate în cod?
   (b) Este corect să utilizăm cheia publică pentru criptarea mesajelor?
   (c) Este corect să utilizăm MD5 pentru stocarea parolelor?
   (d) In cazul cel mai nefavorabil, un atac de tip brute force pentru o cheie de 512 biți necesită 2^{256} încercări.
3. Sistemul de criptare ElGamal.
   (a) (0,2p) Descrieți criptosistemul ElGamal.
   (b) (0,4p) Fie $g = 2$ un generator pentru $\mathbb{Z}_{29}^*$. Pentru cheia secretă $x = 12$, care dintre cele trei valori reprezintă o cheie publică validă $h : 2, 7, 24$? Argumentați.
   (c) (0,4p) Criptați un mesaj $m \in \mathbb{Z}_{29}^*$ la alegere.
4. (1p = 2 x 0,5p) Răspundeți la următoarele cerințe.
   (a) Două din cele trei module RSA $576077, 571367, 577519$ au un factor comun. Care este acesta?
   (b) Calculați simbolul Legendre al lui 8 modulo factorul comun.
5. (1p = 2 x 0,5p) Prezentați protocolul de schimb de chei Diffie-Hellman. Definiți o problemă dificilă pe care se bazează acesta.
6. (1p = 2 x 0,5p) Prezentați atacul de tip Meet-in-the-Middle. Exemplificați un scenariu de atac, indicând cum/în ce condiții se poate realiza un astfel de atac.
7. (1p - bonus) Pentru un mesaj m se calculează criptarea c folosind un sistem de criptare CCA-sigur și tag-ul $t = H(m)$, unde H este o funcție hash rezistenta la coliziuni. Se transmite pe un canal de comunicație nesecurizat perechea (c, t). Ce puteți spune despre integritatea mesajului m? Discuție.