Capitolul 24

Principii criptografice

Exerciţiul 24.1 *Metoda one-time pad (OTP) cifrează un mesaj m prin aplicarea operaţiei XOR cu o cheie secretă k. Având în vedere că o cheie bună are, statistic, jumătate din biţi zero şi că operaţia XOR cu zero nu modifică nimic, rezultă că metoda OTP lasă jumătate din mesaj în clar. Cu alte cuvinte, prin simpla observare a unui text cifrat cu această metodă, un atacator cunoaşte jumătate din biţii textului clar. Acest lucru înseamnă, de fapt, că metoda OTP este una foarte slabă? Cum poate fi considerat "'perfect" un cifru bloc care cifrează numai jumătate din textul clar?*

Exerciţiul 24.2 *Verificarea semnăturii El Gamal presupune efectuarea operaţiei $a^x b^y \bmod p$ unde a, b sunt fixate iar x, y sunt variabile. Arăţi că numărul de înmulţiri necesare pentru efectuarea acestui calcul este mai mic decât numărul de operaţii necesare pentru a calcula $a^x b^y \bmod p$ prin două exponenţieri succesive.*

Exerciţiul 24.3 *Considerăm două numere prime p şi q. Fie $i_p = p^{-1} \bmod q$ si $i_q = q^{-1} \bmod p$ iar $n = p \cdot q$. Care este valoarea rezultată în urma operaţiei $q \cdot i_q + p \cdot i_p$? Puteţi explica cum poate fi folosită această valoare pentru a reduce stocarea cheii secrete la implementarea RSA CRT?*

Exerciţiul 24.4 *Se doreşte semnarea a două mesaje cu algoritmul de semnătura El Gamal. Cum putem calcula valorile g^{k_1} şi g^{k_2} pentru a produce semnăturile într-un timp mai scurt decât cel necesar pentru a calcula două semnături secvenţiale?*

Exerciţiul 24.5 *Considerăm protocolul Fiat-Shamir unde secretul s este ales astfel încât încât $vs^2 = 1 \bmod n$, v fiind cheia publică. Protocolul este după cum urmează:*

- *Alice alege un r aleator şi îi trimite lui Bob $x = r^2 \bmod n$;*
- *Bob răspunde cu un bit aleator e;*
- *Alice răspunde cu $y = s^e r \bmod n$;*

- *Bob verifică dacă* $y^2 = v^e x \bmod n$.

Arătaţi că valorile rezultate în urma protocolului, adică $\{x, r, y\}$*, definesc o distribuţie ce poate fi simulată fără a-l folosi pe* s*. Explicaţi de ce acest lucru asigură protocolului o securitate foarte bună.*

Exerciţiul 24.6 *Se dă o cutie neagră care rulează algoritmul AES (*12 *runde pentru o cheie de* 192 *biţi); cutia conţine o cheie necunoscută* k *şi acceptă ca parametru un întreg* r *a cărui valoare poate fi setată la* 12, 11 *sau* 10 *de către utilizator. Vi se permite să introduceţi în cutie texte clare după cum doriţi. Cum aţi proceda pentru a ataca această implementare?*

Exerciţiul 24.7 *Un administrator de sistem are o cheie de 100 de biţi pe care doreşte să o împartă celor doi utilizatori în care are încredere în mod egal. El doreşte ca accesul la informaţie să fie posibilă numai când cei doi cooperează. Câti biţi din cheie ar trebui să dea fiecăruia din cei doi utilizatori?*

Exerciţiul 24.8 *Pentru a grăbi verificarea semnăturilor* s_i *de tip RSA a mesajelor* m_i*, se foloseşte următoarea idee: se verifică dacă* $(\prod s_i)^e = \prod hash(m_i) \bmod n$ *unde "hash" reprezintă full domain hash - o schemă de semnătură bazată pe RSA care mai întâi aplică o funcţie hash şi apoi semnătura RSA. Arătaţi că această idee nu este sigură pentru un exponent* e *mic şi propuneţi o contramăsură.*

Exerciţiul 24.9 *De ce următorul context este nesigur? O autoritate de încredere generează un modul RSA* n *a cărui factorizare rămâne secretă. Autoritatea furnizează fiecărui utilizator din sistem o pereche* (e_i, d_i) *aşa încât* $e_i d_i = 1 \bmod \phi(n)$ *unde* $i \neq j \Rightarrow d_i \neq d_j$.

Exerciţiul 24.10 *Să presupunem că cineva trimite mesaje cifrate utilizând DES în modul de operare OFB cu o valoare iniţială secretă (fixată)* IV.

1) Arătaţi cum poate fi efectuat un atac cu text clar pentru a decripta mesajele transmise?

2) Este mai bun modul de operare CFB?

3) Dar modul de operare CBC?

Exerciţiul 24.11 *După ce a studiat protocolul Diffie-Hellman, un tânăr criptograf decide să îl implementeze. Pentru a simplifica implementarea, el hotărăşte să folosească grupul aditiv* $(\boldsymbol{Z}_p, +)$ *în locul grupului multiplicativ* $(\boldsymbol{Z}_p^*, \cdot)$*. În calitate de criptograf cu experienţă, ce credeţi despre acest protocol?*

Exerciţiul 24.12 *Să presupunem că Alice şi Bob folosesc chei publice RSA cu acelaşi modul* n *dar cu exponenţi publici diferiti* e_1 *şi* e_2.

1) Arătaţi că Alice poate decripta mesajele trimise lui Bob;

2) Arătaţi că Alice poate decripta mesaje trimise către Alice şi Bob dacă $gcd(e_l, e_2) = 1$.

Exerciţiul 24.13 *Presupunem că $n = p \cdot q$, unde p si q sunt numere prime distincte.*

1) Calculaţi $S = n + 1 - \phi(n)$.

2) Care sunt rădăcinile ecuaţiei $x^2 - Sx + n$? Daţi expresiile acestor rădăcini şi explicaţi cum pot fi găsite p şi q cu ajutorul unui simplu algoritm pentru calculul rădăcinilor pătrate întregi?

3) Factorizaţi n în următoarele două cazuri:

a) $n = 667, \phi(n) = 616$;

b) $n = 15049, \phi(n) = 14800$.

Exerciţiul 24.14 *Să construim un MAC folosind modul CFB de implementare, în loc de modul CBC: fiind date blocurile de text clar $\alpha_1, \ldots, \alpha_n$, definim vectorul de iniţializare $\beta_0 = \alpha_1$. Apoi cifrăm secvenţa de blocuri $\alpha_2, \ldots, \alpha_n$ după formulele:*

$$\beta_i = \alpha_{i+1} \oplus E(\beta_{i-1}; K).$$

În final, $MAC(\alpha_1 || \ldots \alpha_n) = E(\beta_{i-1}; K)$. Arătaţi că acesta este identic cu CBC MAC.