Examen crypto

Iuga Stefan - 332

May 21, 2020

1 Subiecte netratate

2(b), 2(c), 2(d), 2(e), 3(d), 3(f), 4(c)

2 Rezolvari

1. (a) Cheia K este o cheie random si cel putin la fel de lunga ca mesajul transmis.
   (b) Daca mesajul si cheia sunt identice, operatia XOR intoarce un mesaj compus doar din 0-uri. Mesajul nu poate fi descifrat.
2. (a) Mesajul criptat c reprezinta concatenarea blocurilor criptate c_1, c_2, c_3 unde $c_i = F_k(m_i \oplus (ctr + i)), i \in \{1, 2, 3\}$
3. (a) Securitatea parolelor depinde de salt-ul folosit. Daca salt-ul este unul lung, diferit pentru fiecare client si stocat alt undeva decat parola, atunci metoda poate fi sigura. MD5 nu este recomandat, in general, pentru stocarea parolelor deoarece este un algoritm foarte rapid iar metoda brute-force este eficienta pentru aflarea acestora.
   (b) $G(x) = x^2 \mod x \Rightarrow G(x) = 0 \forall x$
   Cum $G(x)$ este 0 tot timpul, el nu este random.
   (c) Criptarea fluida presupune generarea unei secvente de biti folosind G iar apoi XOR-area mesajului cu aceasta secventa.

$$c = m \oplus G(x) = m \oplus (x^2 \mod x) = m \oplus 0 = m$$

   Cum G e tot timpul 0, mesajul criptat c va fi chiar mesajul in clar m.
   (e) Protocolul este vulnerabil unui atac Man-in-the-Middle. O solutie poate fi folosirea unor chei generate de un CA pentru semnarea mesajelor.
   (g) Este incalcat principiul lui Kerckhoffs. Un sistem bun nu are nevoie de un NDA pentru a il tine secret, el functioneaza perfect si atunci cand algortimul este public.

(h) Sistemul prezent incalca urmatoarele obiective:

i. Confidentialitatea: prin folosirea unui algoritm nerecomandat pentru pastrarea parolelor

ii. Disponibilitatea: un atac Man-in-the-Middle poate intarzia transmisisa in timp util a datelor

iii. Autentificarea: lipsa autentificarii permite atacul Man-in-the-Middle

4. (a) N in reprezentare decimala este: 437193815245112290266046121597579180948375300191673990816835546146297683370344486861551838471835558876426406073953181320837746931157832411801246591017315418380680496618870797988842839214087714455833172607937845783237469778690366308719633937342116994347322862944406591197171611951438813042083102149017043257829922345957048339062329261006916850192497142355135902606726005162896328829187750876173297807773534142652349572185766272153579933980509742518141185857445145890283784188800918043073911199364085199236962965710609940558051978936412795262515966866892954399204189062172544199831505882279856902511940522422528183829 6

Ultimele 3 cifre ale lui N formeaza numarul 296, iar acesta este divizibil cu 8, atunci si N este divizibil cu 8 (2^3).

Cum N nu este un produs de doar 2 numere prime, el nu poate fi folosit ca parametru.

(b) Un punct ce apartine curbei eliptice are invers (curba este simetrica).

- Pentru punctul (8,10)

$$\begin{aligned} 10^2 &\mod 29 = 8^3 + 17 * 8 + 3 \mod 29 \\ 100 &\mod 29 = 512 + 136 + 3 \mod 29 \\ 13 &\mod 29 = 13 \mod 29 \end{aligned}$$

Punctul (8,10) apartine curbei $\Rightarrow$ are invers/simetric pe curba
Inversul: $-(8,10) \mod 29 = (8,-10) \mod 29 = (8,19) \mod 29$
Verificare:

$$\begin{aligned} 19^2 &\mod 29 = 8^3 + 17 * 8 + 3 \mod 29 \\ 361 &\mod 29 = 512 + 136 + 3 \mod 29 \\ 13 &\mod 29 = 13 \mod 29 \end{aligned}$$

- Pentru punctul (8,11)

$$\begin{aligned} 11^2 &\mod 29 \neq 8^3 + 17 * 8 + 3 \mod 29 \\ 121 &\mod 29 \neq 512 + 136 + 3 \mod 29 \\ 5 &\mod 29 \neq 13 \mod 29 \end{aligned}$$

Punctul (8,11) nu apartine curbei

(d) Curba eliptica W-25519 recomandata de NIST

$$y^2 \equiv x^3 + ax + b \mod p$$
$$p = 2^{255} - 19$$
$$a = 19298681539552699237261830834781317975712544997444273427339909597334573241639236$$
$$b = 55751746669818908907645289078257140818716241103727901012315294400837956729358436$$