Napredni operacijski sustavi — Međuispit Rješenja

29. travnja 2021.

1. (a) Prema tipu poruke.
   (b) Ne.
   (c) `close(fd[pisanje]), close(std_in), dup(fd[čitanje]), close(fd[čitanje])`
   (d) Cijeli protokol će zatajiti.
   (e) Primitak poruka `ZAHTJEV` i `ODGOVOR`.
   (f) $2 * (N - 1)$.

2. (a) Skica koja pokazuje komunikaciju, pravilno ažuriranje logičkih satova i sadržaj poruka.
   (b) (P_1, P_3, P_2)
   (c) P1: 15 ili 16, P2: 16, P3: 15 ili 16

3. (a) $3 * (4 - 1) * (1 + 2 + 3 + 4) = 90$
   (b) $9Z + 3O + 9I = 21$, $3Z + 9O + 3I = 15$
   $8Z + 6O + 8I = 22$, $2 * 3Z + 8O + 2 * 3I = 20$
   $7Z + 9O + 7I = 23$, $3 * 3Z + 7O + 3 * 3I = 25$
   $6Z + 12O + 6I = 24$, $4 * 3Z + 6O + 4 * 3I = 30$

4. (a) Pomoću digitalnog potpisa.
   (b) Ne možemo jer potpis može biti vezan uz više identiteta koji dijele isti ključ.
   (c) Iz $C = P \oplus K$ imamo $K = C \oplus P = 0101$.
   (d) Duljina ključa mora biti veća ili jednaka duljini jasnog teksta, ključ mora biti iskorišten samo jednom.
   (e) $3DES(P, K_1, K_2, K_3) = DES(DES^{-1}(DES(P, K_1), K_2), K_3)$.
   (f) Kada su svi ključevi jednaki.

5. (a) ECB, OFB, CTR.

(b) Galoisovo polje ili $GF(2^8)$.

(c) Neka je OFB blok toka za kriptiranje. S obzirom da koristimo isti inicijalizacijski vektor IV, vrijedi da je OFB jednak za prvi i drugi tok pa imamo:

$$C_1 = M_1 \oplus OFB$$
$$C_2 = M_2 \oplus OFB$$

Iz toga vrijedi da je $C_1 \oplus C_2 = M_1 \oplus M_2$. Iz teksta zadatka ne znamo je li $M = M_1$ ili $M = M_2$, no to nije ni bitno jer $M' = C_1 \oplus C_2 \oplus M = M_1 \oplus M_2 \oplus M$ sigurno predstavlja prvi blok jasnog teksta onog drugog toka.

$$\begin{aligned}
C_1 &= (\texttt{10 39 23 3C 26})_{hex} \\
&= (\texttt{00010000 00111001 00100011 00111100 00100110})_2 \\
C_2 &= (\texttt{19 3C 23 30 26})_{hex} \\
&= (\texttt{00011001 00111100 00100011 00110000 00100110})_2 \\
C_1 \oplus C_2 &= (\texttt{09 05 00 0C 00})_{hex} \\
&= (\texttt{00001001 00000101 00000000 00001100 00000000})_2 \\
M &= (\texttt{45 6C 76 69 73})_{hex} \\
&= (\texttt{01000101 01101100 01110110 01101001 01110011})_2 \\
&= (\texttt{E l v i s})_{ascii} \\
M' &= C_1 \oplus C_2 \oplus M \\
&= (\texttt{4C 69 76 65 73})_{hex} \\
&= (\texttt{01001100 01101001 01110110 01100101 01110011})_2 \\
&= (\texttt{L i v e s})_{ascii}
\end{aligned}$$

Stoga, napadač može zaključiti da je prvi blok jasnog teksta drugog toka jednak

$$\begin{aligned}
M' &= (\texttt{01001100 01101001 01110110 01100101 01110011})_2 \\
&= (\texttt{L i v e s})_{ascii}
\end{aligned}$$

Primjetite da smo odmah, bez računanja, mogli zaključiti da se slova “v” i “s” nalaze u drugoj poruci! Da bi zadatak bio priznat dovoljno je naći binarnu ili hex reprezentaciju od M', nije nužno zaključiti o kakvom je ASCII tekstu riječ.

Zbog greške, u tablici nije navedeno slovo "e" pa su se priznavala rješenja bez istog.

6. (a) $\varphi(N) = |\mathbb{Z}_N^*|$ (ovo je dovoljno), odnosno broj prirodinih brojeva manjih od N koji su relativno prostih s N.
   Sljedeća rješenja nisu ispravna jer ne predstavljaju definiciju.
   i. $\varphi(p \times q) = (p-1) \times (q-1)$
   ii. $a^{\varphi(N)} = 1 \mod N$

   (b) S obzirom da je $\varphi(N) = (p-1) * (q-1)$ paran broj, da bi e bio relativno prost s $\varphi(N)$, e nužno mora biti neparan.

   (c) (1) (0.5) $\varphi(N) = \varphi(65) = \varphi(5 * 13) = (5-1) * (13-1) = 48$
   (2) (0.5) $5 * 29 = 145 = 1 + 3 * 48$
   (3) (0.5) $4^5 = 1024 \mod 65 = 49 \mod 65$.
   Rješenja gdje se umjesto modulo N koristilo modulo $\varphi(N)$ ne priznaju se.
   (4) (1.5) $29 = 16 + 8 + 4 + 1 = (11101)_2$

i	4	3	2	1	0
$a[i]$	1	1	1	0	1
d	17	38	43	29	**62**

   Rješenja gdje se umjesto modulo N koristilo modulo $\varphi(N)$ ne priznaju se.

7. (4 boda ukupno) Razmatramo sustav digitalnog potpisa.

   (a) Sustav digitalnog potpisa je uređena trojka: (G, S, V), gdje je G algoritam generiranja para ključeva pk i sk, $S(m, sk)$ algoritam potpisivanja, $V(m, \sigma, pk)$ algoritam verifikacije.
   Bez navođenja algoritma generiranja para ključeva nisu se mogli dobiti svi bodovi.

   (b) Autentičnost i integritet.

   (c) Nasumično odaberemo $x \in \mathbb{Z}_N$ i definiramo $y = x^e$. Sada je x ispravan potpis za poruku y.

   (d) U praksi je javni eksponent $e \in \mathbb{Z}_{\varphi(N)}^*$ znatno manji od privatnog eksponenta $d \in \mathbb{Z}_{\varphi(N)}^*$ pa ćemo sa znatno manjim brojem množenja izračunati $m = \sigma^e$ u odnosu na $\sigma = m^d$ za poruku $m \in \mathbb{Z}_N^*$.