MKC-NBS: Úkol č. 1

Filip Paul

Kryptografie

17.02.2022

Bloková šifra v režimu CBC:

1. **Zadání:**
   Mějme zprávu Z = (13, 4, 9), kde jednotlivá čísla jsou bloky zprávy. Tuto zprávu zašifrujte v režimu CBC pro inicializační vektor IV = 6. Vypočítaný kryptogram pro kontrolu dešifrujte. Šifrování E a dešifrování D je dáno substitucemi podle tabulky 1. K provedení operací XOR si dekadická čísla převeďte na čtyřbitová čísla. Pro daný provozní režim nakreslete diagramy podle první přednáškové prezentace (snímek č. 21), přičemž v datových blocích schématu uveďte dekadicky i binárně hodnotu příslušného vstupu, či výstupu.

Table 1: Šifrovací substituce y = E(x,K)

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Y	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

2. **Vypracování:**

Výpočet pečeti HMAC

1. **Zadání:**
   Mějme zprávu Z = (13, 4, 9), kde jednotlivá čísla jsou bloky zprávy. Pro tuto zprávu vypočítejte technikou HMAC pečeť P. Pečetící klíč K = 7, konstanta $C_1 = 13$ a $C_2 = 8$. K provedení operací XOR si dekadická čísla převeďte na čtyřbitová čísla. Hešovací funkce H je definována následovně:

   $h = \left(\sum_{i=1}^{t} a^i \cdot v_i\right) mod 17$

   kde hešovací konstanta a = 11, v_i je i-tý blok hešovaného vstupu a t počet bloků na vstupu. V prvém hešování tedy bude t = 4, protože první blok je výsledek xorování klíče a konstanty a další bloky jsou bloky zprávy. Ve druhém hešování bude t = 2. Pečetí P je výstup z druhého hešování, tj. P = h_2.

2. **Vypracování:**

RSA podpis

1. **Zadání:**
   Byla Vám doručena zpráva Z = (13, 4, 9), jejíž RSA podpis DS = 5. Ověřte, zda je tato zpráva autentická. Znáte veřejný ověřovací klíč udávaného autora VK = 3, jeho modulus n = 33 a víte, že byla použita hešovací funkce H ze 2. příkladu.

2. **Vypracování:**