Üzenethitelesítés

2011. február 25.

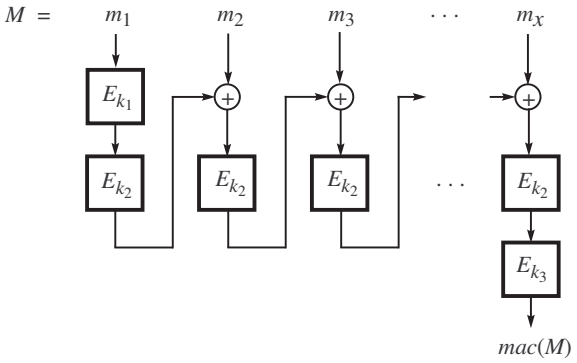
Feladatok

1. feladat

Tekintsük a az 1. ábrán illusztrált CBC-MAC sémát. Tegyük fel, hogy valamely $M = m_1|\ldots|m_x$ és $M' = m'_1|\ldots|m'_y$ üzenetre $mac(M) = mac(M')$, ahol $m_x \neq m'_y$. Mutassuk meg, hogy ekkor bármely $\tilde{m}$ blokkra teljesül a következő:

$$mac(m_1|\ldots|m_{x-1}|\tilde{m}) = mac(m'_1|\ldots|m'_{y-1}|\tilde{m} \oplus m_x \oplus m'_y)$$

(azaz, ha egy ütközést találunk, akkor tetszőlegesen sok ütközést konstruálhatunk belőle).



1. ábra. A 3DES-MAC séma

2. feladat

Tekintsük a következő üzenet-hitelesítési sémát: Az üzenetet 128 bites blokkokra osztjuk (ha kell az utolsó blokkot nullákkal egészítjük ki egy teljes blokkra), majd az így nyert blokkokat XOR-oljuk. A 128 bites X XOR összeget az AES blokkrejtjelezővel kódoljuk, és így kapjuk az eredeti üzenet MAC értékét.

Miért nem biztonságos ez a séma?

3. feladat

Hitelesített rejtjelezést végzünk a következő módon: az üzenetet hash-eljük, majd az üzenetet és a hash-t együtt rejtjelezzük OFB módban. Formálisan, az m üzenethez tartozó hitelesített és rejtjelezett üzenet a $c = E_K(m|h(m))$, ahol a rejtjelezés OFB módban történik.

Mutassuk meg, hogy ha a támadó hozzájut egy (m, c) nyílt szöveg – rejtett szöveg párhoz, akkor tetszőleges m' üzenethez elő tudja állítani a $c' = E_K(m'|h(m'))$ hitelesített rejtjelezést!

Megoldások

1. feladat

Legyen $D_{k_2}(D_{k_3}(mac(M))) = d$.

Az M üzenet utolsó blokkjának feldolgozásánál, az m_x-hez XOR-olt érték: $d \oplus m_x$.

Hasonlóan, az M' üzenet utolsó blokkjának feldolgozásánál, az m'_y-hoz XOR-olt érték: $d \oplus m'_y$, mert $mac(M') = mac(M)$.

Az $m_1|m_2|\ldots|m_{x-1}|\tilde{m}$ üzenet esetében a MAC érték: $E_{k_3}(E_{k_2}(d \oplus m_x \oplus \tilde{m}))$

Az $m'_1|m'_2|\ldots|m'_{y-1}|\tilde{m}\oplus m_x \oplus m'_y$ üzenet esetében a MAC érték: $E_{k_3}(E_{k_2}(d \oplus m'_y \oplus \tilde{m} \oplus m_x \oplus m'_y)) = E_{k_3}(E_{k_2}(d \oplus \tilde{m} \oplus m_x))$

A két érték valóban megegyezik.

2. feladat

Könnyű két olyan üzenetet találni, melyeknek ugyanaz lesz a MAC értéke. Vegyünk egy m üzenetet, s legyen ennek blokkjainak a konstrukció szerinti XOR összege X. Az m' üzenetet úgy állítjuk elő m-ből, hogy annak páros számú blokkjában az azonos pozícióban álló biteket invertáljuk. Az így nyert m' XOR összege szintén X, s ezért m és m' MAC értéke megegyezik.

3. feladat

Lényegében kulcsfolyamos rejtjelezést végzünk, s tudjuk, hogy ekkor ismert nyílt szöveg – rejtett szöveg pár esetén kiszámolható a k kulcsfolyam: $m \to h(m) \to k = c \oplus (m|h(m))$. Ezzel a kulcsfolyammal tetszőleges más üzenet kódolható: $m' \to h(m') \to c' = (m'|h(m')) \oplus k$.