Blokk-rejtjelezési módok

2011. február 24.

Feladatok

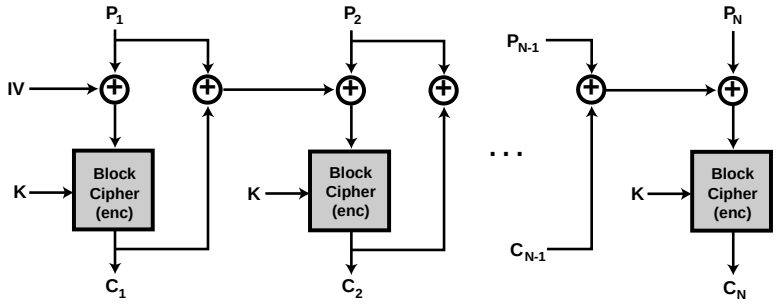
1. feladat

Legyen $P = P_1|P_2|\ldots|P_N$ egy N blokkból álló nyíltszöveg. P-t CBC módban rejtjelezzük egy K kulccsal és egy IV kezdeti változóval. Az eredmény legyen az N blokkból álló $C = C_1|C_2|\ldots|C_N$ rejtettszöveg. Tegyük fel, hogy egy támadó megszerzi P-t és C-t, valamint megfigyel egy másik, M blokkból álló $C' = C'_1|C'_2|\ldots|C'_M$ rejtettszöveget, melyről azt is tudja, hogy szintén CBC módot használva ugyanazzal a K kulccsal de különböző kezdeti változóval állították elő, mint C-t. Tegyük fel továbbá, hogy C_i megegyezik C'_j-vel valamely i-re és j-re, ahol $1 < i \leq N$ és $1 < j \leq M$.

- Mutassa meg, hogy ekkor a támadó meg tudja fejteni P'_j-t (azaz a C' rejtettszöveghez tartozó nyíltszöveg j. blokkját).
- Mekkora annak a valószínűsége, hogy a támadó által megfigyelt M blokkból álló C' legalább egy blokkja megegyezik a támadó által ismert, N blokkból álló C valamely blokkjával, ha a blokkméret n bit és C minden blokkja különböző?

2. feladat

Az 1. ábra egy blokk rejtjelező (pl. DES) használatát mutatja PCBC (Plain and Cipher Block Chaining) módban.



1. ábra. Blokk rejtjelező használata PCBC módban

- Adja meg a dekódoló sémáját.
- Tegyük fel, hogy a C_i és C_{i+1} blokkokat egy támadó felcseréli egymással. Mutassa meg, hogy ennek csak a P_i és P_{i+1} nyílt blokkokra van hatása.
- Önszinkronizáló-e a PCBC mód? Miért?

3. feladat

Rejtjelezett üzeneteinket egy 10^{-4} bit hiba arányú csatornán továbbítjuk. Mekkora átlagos bit hiba arányt figyelhetünk meg a dekódoló kimenetén ha

- AES-t használunk CBC módban?
- AES-t használunk CFB módban, és 8 bites karaktereket rejtjelezünk?
- AES-t használunk CTR módban, és teljes blokkokat rejtjelezünk?

4. feladat

Egy n blokkból álló $M = (m_1, m_2, \ldots, m_n)$ üzenetet CTR módban rejtjelezünk és eredményül a $C = (c_1, c_2, \ldots, c_n)$ rejtjeles üzenetet kapjuk, amit tárolunk. Később kiderül, hogy az i. blokkot nem kell tárolnunk, ezért C-t dekódoljuk, az i. blokkot töröljük, és az így kapott $M' = (m_1, m_2, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n)$ üzenetet újra kódoljuk. A második kódolás során a számlálót ugyanattól az értéktől indítjuk, mint az első kódolásnál, és a kulcs is ugyanaz. Legyen a második kódolás eredménye $C' = (c'_1, c'_2, \ldots, c'_{n-1})$. (Vegyük észre, hogy minden $1 \leq t < i$ esetén $c'_t = c_t$, ezért lényegében az első $i - 1$ blokkot nem is kell újra kódolnunk.)

Tegyük fel, hogy egy támadó hozzáfér C-hez és C'-höz, és megszerzi a törölt m_i-t is. Fenyegeti-e veszély az M' üzenet titkosságát?

Megoldások

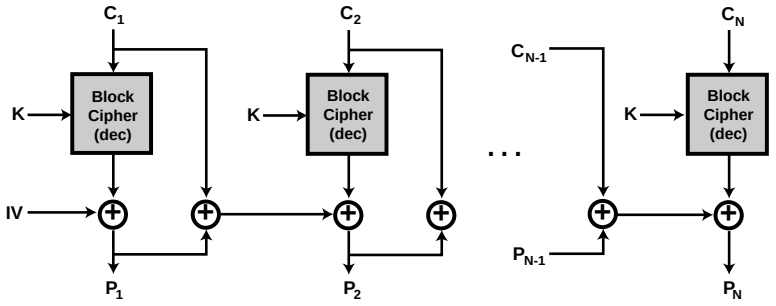
1. feladat

Tudjuk, hogy $C_i = E_K(C_{i-1} \oplus P_i)$ és $C'_j = E_K(C'_{j-1} \oplus P'_j)$. Mivel $C_i = C'_j$, ezért $C_{i-1} \oplus P_i = C'_{j-1} \oplus P'_j$. Ebből $P'_j = C'_{j-1} \oplus C_{i-1} \oplus P_i$, ahol C'_{j-1}, C_{i-1}, P_i ismertek a támadó számára.

Annak valószínűsége, hogy C' első blokkja megegyezik C valamelyik blokkjával: $N2^{-n}$. Annak valószínűsége, hogy C' első blokkja nem egyezik meg C egyetlen blokkjával sem: $1 - N2^{-n}$. Annak valószínűsége, hogy C' egyetlen blokkja sem egyezik meg C egyetlen blokkjával sem: $(1 - N2^{-n})^M$. Annak valószínűsége, hogy C' legalább egy blokkja megegyezik C valamely blokkjával: $1-(1-N2^{-n})^M$.

2. feladat

A dekódoló sémáját a 2. ábra mutatja.



2. ábra. A PCBC mód dekódolási sémája

Az $i.$ és az $(i+1).$ rejtjeles blokk felcserélésének az $(i-1).$ nyílt blokkra nyílván nincs hatása, az $i.$ és az $(i+1).$ nyílt blokkra pedig nyílván van hatása. Azt kell megmutatni, hogy az $(i+2).$ nyílt blokkra a cserének már nincsen hatása. Írjuk fel az $(i+2).$ nyílt blokkot az eredeti esetben és akkor amikor a rejtjeles blokkokat felcseréljük:

$$\begin{aligned} P_{i+2} &= D_K(C_{i+2}) \oplus C_{i+1} \oplus P_{i+1} \\ &= D_K(C_{i+2}) \oplus C_{i+1} \oplus D_K(C_{i+1}) \oplus C_i \oplus P_i \\ &= D_K(C_{i+2}) \oplus C_{i+1} \oplus D_K(C_{i+1}) \oplus C_i \oplus D_K(C_i) \oplus C_{i-1} \oplus P_{i-1} \end{aligned}$$

és

$$\begin{aligned} P'_{i+2} &= D_K(C_{i+2}) \oplus C_i \oplus P'_{i+1} \\ &= D_K(C_{i+2}) \oplus C_i \oplus D_K(C_i) \oplus C_{i+1} \oplus P'_i \\ &= D_K(C_{i+2}) \oplus C_i \oplus D_K(C_i) \oplus C_{i+1} \oplus D_K(C_{i+1}) \oplus C_{i-1} \oplus P_{i-1} \end{aligned}$$

Látható, hogy $P_{i+2} = P'_{i+2}$

A PCBC mód nem önszinkronizáló, azaz egy bit hiba az $i.$ rejtjeles blokkban elrontja az $i.$ és az összes azt követő nyílt blokk dekódolását. Könnyen látható, hogy az $i.$ nyílt blokk elromlik. Legyen a hibás $i.$ rejtjeles blokk C'_i és a hibás $i.$ nyílt blokk P'_i. Ekkor $P'_{i+1} = D_K(C_{i+1}) \oplus C'_i \oplus P'_i$. Mivel P'_i pénzfeldobás sorozat, ezért nagy valószínűséggel $C'_i \oplus P'_i \neq C_i \oplus P_i$, azaz nagy valószínűséggel az $(i+1).$ nyílt blokk is hibás lesz. Most bebizonyítjuk, hogy ha a $j.$ blokk hibás (ahol $j > i$), akkor a $j+1.$ blokk is hibás lesz, s ebből következik az állítás. Legyen a hibás $j.$ blokk P'_j. Ekkor $P'_{j+1} = D_K(C_{j+1}) \oplus C_j \oplus P'_j \neq D_K(C_{j+1}) \oplus C_j \oplus P_j = P_{j+1}$.

3. feladat

CBC módban egy bit hiba az i. rejtjeles blokkban elrontja az i. nyílt blokk bitjeinek felét (átlagosan) és a következő nyílt blokk egy bitjét. Mivel az AES blokk mérete 128 bit, ezért a dekódoló kimenetén megfigyelt bit hiba arány: $(64 + 1) \cdot 10^{-4} = 65 \cdot 10^{-4}$.

CFB módban egy bit hiba az i. rejtjeles karakterben elrontja az i. nyílt karakter egy bitjét majd az azt követő n/s nyílt karakter bitjeinek átlagosan felét, ahol n a rejtjelező blokkmérete és s a karakterek mérete bitben mérve. Jelen esetben $n = 128$, $s = 8$, ezért a megfigyelt bit hiba arány: $(1 + \frac{128}{8} \cdot 4) \cdot 10^{-4} = 65 \cdot 10^{-4}$.

CTR módban nincs hibaterjedés, ezért a megfigyelt bit hiba arány a dekódoló kimenetén 10^{-4}.

4. feladat

Legyen a számlálóból előállított kulcsblokkok sorozata $k_1, k_2, \ldots$. Ekkor $c_t = m_t \oplus k_t$ minden $1 \leq t \leq n$ esetén, valamint $c'_i = m_{i+1} \oplus k_i$, $c'_{i+1} = m_{i+2} \oplus k_{i+1}$, stb.

A támadó a következőket tudja kiszámolni:

$m_i, c_i = m_i \oplus k_i \rightarrow k_i = c_i \oplus m_i$

$k_i, c'_i = m_{i+1} \oplus k_i \rightarrow m_{i+1} = c'_i \oplus k_i$

$m_{i+1}, c_{i+1} = m_{i+1} \oplus k_{i+1} \rightarrow k_{i+1} = c_{i+1} \oplus m_{i+1}$

$k_{i+1}, c'_{i+1} = m_{i+2} \oplus k_{i+1} \rightarrow m_{i+2} = c'_{i+1} \oplus k_{i+1}$

$\ldots$

A támadó tehát dekódolni tudja az $m_{i+1}, m_{i+2}, \ldots, m_n$ blokkokat, azaz komoly veszély fenyegeti M' titkosságát ha $i < n$.