Sicurezza nelle Reti

Appello del 14 Luglio 2006

SOLUZIONE

QUESITO 1 — PUNTI: 8

In un cifrario C esistono un messaggio m ed un crittogramma c tali che Prob($M = m$) = p, con $p < 1/4$, e Prob(M=m|C=c) = 1–p. Spiegare se C può essere un cifrario perfetto e le conseguenze per un crittoanalista per la coppia (m, c) indicata.

Affinché il cifrario sia perfetto bisogna che $p = 1 - p$. Questa uguaglianza non è soddisfatta per p < ¼ e perciò il cifrario non è perfetto. Questo implica che se l'avversario vede passare in rete il crittogramma c allora può concludere che è stato trasmesso il messaggio m con una probabilità $1 - p$. Siccome questa probabilità è maggiore di p, la probabilità con cui viene trasmesso m, allora l'avversario ha guadagnato dall'osservazione del testo cifrato maggiori informazioni su m.

QUESITO 2 — PUNTI: 10 (8, 2)

A e B utilizzano un crittosistema simmetrico $E()$ ed una funzione hash con chiave $h()$. A e B utilizzano inoltre le chiavi segrete condivise K e K' con il crittosistema e la funzione hash, rispettivamente. Infine A e B utilizzano un meccanismo contatore-finestra (come quello di IPsec) di supporto ad un servizio anti-replay. Supponendo che il formato dei messaggi sia m = (c, x, d), con x valore del contatore del mittente, specificare quale, o quali, dei seguenti casi fornisce il servizio anti-replay:

1. c = E(K, m); d = h(K′, x)
2. c = E(K, m || x); d = h(K′, x)
3. c = E(K, m); d = h(K′, c || x)

In caso di soluzioni equivalenti, indicare quella che permette di realizzare il servizio anti-replay con il minore carico computazionale dal punto di vista del ricevitore.

La prima soluzione non garantisce l'anti-replay perché m ed x non sono "indissolubilmente" (crittograficamente) legati tra di loro. La seconda e la terza soluzione garantiscono anti-replay con una differenza dal punto di vista dell'overhead computazionale. Nella seconda, la verifica dell'anti-replay richiede la decifratura del messaggio. Perciò saranno inutilmente decifrati anche i messaggi destinati ad essere scartati. Nella terza, la verifica viene fatta sul testo cifrato. Quindi la decifratura verrà eseguita solo dei messaggi che sono accettati.

QUESITO 3 — PUNTI: 12 (4, 4, 4)

Con riferimento al sistema RSA, il candidato, con precisione matematica e proprietà di linguaggio,

1. descriva gli algoritmi di generazione della chiave, di cifratura e di decifratura;
2. ne discuta la "sicurezza" (relazione tra RSA ed un problema complesso); ed infine
3. illustri perché il riutilizzo del modulo può portare ad un *common modulus attack.*

Vedere materiale didattico.