LAUREA SPECIALISTICA IN INGEGNERIA INFORMATICA

SICUREZZA NELLE RETI

Appello del 16 Gennaio 2005

Nome e Cognome_____ **Matricola**_____

ESERCIZIO 1 — PUNTI: 8

(A.A. 2004-05). Il candidato spieghi con precisione matematica e proprietà di linguaggio il legame tra n, il numero di bit di un blocco, e k, il numero di bit di una chiave, in un *true random cipher*. Il candidato discuta inoltre le difficoltà pratiche legate alla realizzazione di tale tipo di cifrario.

(A.A. 2005-06). Il candidato dimostri che se un cifrario è perfetto allora il numero delle chiavi deve essere maggiore o uguale al numero dei messaggi.

ESERCIZIO 2 — PUNTI: 14 (4, 5, 5)

Si consideri il seguente protocollo di distribuzione delle chiavi orientato a stabilire una chiave di sessione $K_{AB} = h(k_a, k_b)$ tra i processi A e B, con h funzione hash one-way:

M1 $A \rightarrow B$: $E_{e_b}(k_a, A)$ M2 $B \rightarrow A$: $E_{e_a}(k_a, k_b)$ M3 $A \rightarrow B$: $E_{e_b}(k_b)$	• E: cifrario asimmetrico; • k_a e k_b: quantità segrete scelte rispettivamente da A e B; • e_a ed e_b: le chiavi pubbliche, rispettivamente, di A e B

Si assuma che

(i) le quantità k_a e k_b non siano mai riutilizzate;

(ii) ciascun processo conosca la chiave pubblica dell'altro, il candidato risponda alle seguenti domande motivando le risposte.

Quesito A. Il protocollo garantisce la confidenzialità della chiave di sessione?

Quesito B. Analizzando il protocollo con la logica BAN, il candidato discuta se il protocollo garantisce le proprietà di key authentication e di key confirmation specificando le ipotesi sotto le quali tali proprietà valgono.

Si assuma adesso che l'ipotesi (i) non sia più verificata.

Quesito C. Il candidato verificata, quali conseguenze possono scaturire.

ESERCIZIO 3 — PUNTI: 8 (4, 4)

Si consideri il protocollo (semplificato) di identificazione di WEP (IEEE 802.11) per mezzo del quale una mobile station MS si identifica presso un access point AP per avere accesso alla rete (sia k una chiave segreta su 104 bit, condivisa tra MS ed AP):

1. MS invia una richiesta di identificazione ad AP.
2. AP genera in modo casuale una challenge χ su 128 bit e la invia a MS.
3. MS genera in modo casuale un vettore di inizializzazione v su 24 bit, calcola la response $\rho = E_{k,v}(\chi)$ ed invia ad AP la frame $\langle v, \rho \rangle$.
4. Alla ricezione della frame, AP estrae le quantità v e ρ, e verifica se $\chi = D_{k,v}(\rho)$. Se la verifica ha esito positivo, AP permette ad MS l'accesso alla rete; altrimenti, vieta tale accesso.

Il cifrario utilizzato è definito in Figura 1, dove m_i e c_i sono, rispettivamente, l'i-esimo byte del testo in chiaro e del testo cifrato. La chiave k ed il vettore di inizializzazione v sono concatenati per formare il seme s del generatore random sicuro di byte detto *Key Sequence Generator* (*KSG*). Con z_i si denota l'i-esimo byte del *key stream* generato da KSG.

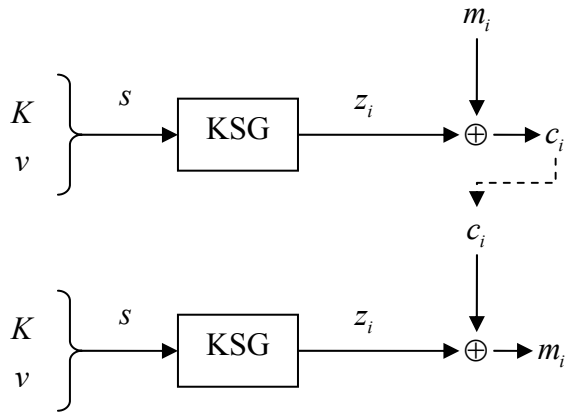

Figura 1. Il cifrario di WEP.

Si assuma che la chiave K è fissa ed unica per tutte le mobile station appartenenti alla rete.

Quesito A. Il candidato discuta se il protocollo WEP garantisce l'identificazione oppure no ovvero se un avversario (passivo) può impersonare una mobile station della rete.

Si assuma adesso di modificare il protocollo in modo tale che, al passo 2, AP generi in modo causale il vettore di inizializzazione v e lo invii in chiaro a MS insieme alla challenge[1].

Quesito B. Il candidato definisca un dictionary attack contro questa variante del protocollo di identificazione e valuti la dimensione in byte del dizionario.

[1] Si noti che adesso non è più necessario trasmettere v insieme alla response.

LAUREA SPECIALISTICA IN INGEGNERIA INFORMATICA

SICUREZZA NELLE RETI

Appello del 16 Gennaio 2006

SOLUZIONE

ESERCIZIO 1

(**A.A. 2004-05**). Con n bit si hanno 2^n possibili blocchi in chiaro. Un true random cipher realizza tutte le possibili permutazioni, cioè $2^n!$ e richiede perciò $k = \log_2(2^n!)$ che risulta essere $O(n2^n)$.

(**A.A. 2005-06**). Per prima cosa si osserva che affinché il cifrario sia invertibile è necessario che il numero di testi cifrati N_c sia maggiore o uguale al numero di testi in chiaro N_m, $N_c \geq N_m$. La dimostrazione è per assurdo. Supponiamo che il numero di chiavi N_k sia minore del numero N_m di messaggi in chiaro, $N_k < N_m$. Ne segue quindi che $N_k < N_c$.

Sia m un messaggio che ha probabilità non nulla di essere trasmesso, $P(M = m) \neq 0$. Dalla condizione $N_k < N_c$ segue che esiste un crittogramma c che non è immagine di m. Perciò, $P(M = m, C = c) = 0 \neq P(M = m)$, contro l'ipotesi che il cifrario sia perfetto.

ESERCIZIO 2

Quesito A. Il protocollo garantisce la confidenzialità. Per determinare il valore di K_{AB} è necessario conoscere le quantità k_a e k_b. Tuttavia queste quantità viaggiano in rete in forma cifrata.

Quesito B. Il protocollo è una versione semplificata del protocollo Needham-Schroeder a chiave pubblica. Il protocollo garantisce sia la key autentication sia la key confirmation. Formalmente,

$$A \mid\equiv B \mid\equiv A \overset{k_b}{\rightleftharpoons} B \text{ e } B \mid\equiv A \mid\equiv A \overset{k_a}{\rightleftharpoons} B.$$

Quesito C. Se l'ipotesi (i) non è verificata, il protocollo non garantisce la proprietà di key authentication. Supponiamo che la quantità k_a sia riutilizzata da A e che un avversario M abbia registrato i messaggi M1 ed M2 relativi all'esecuzione del protocollo in cui k_a è stata utilizzata la prima volta. L'avversario M potrebbe eseguire il seguente attacco:

- l'avversario M induce A ad iniziare una nuova istanza del protocollo con B;
- quando A invia il messaggio M1' relativo alla nuova esecuzione del protocollo, contenente la quantità riutilizzata k_a, l'avversario M determina che M1=M1', e risponde con M2. Alla ricezione di questo messaggio il processo A crede di parlare effettivamente con B.

Si noti che questo attacco ha come effetto collaterale il riutilizzo della vecchia chiave di sessione K_{ab} (la quantità k_b è contenuta nel messaggio M2 replicato da M). L'avversario M potrebbe non conoscere tale chiave ma potrebbe comunque replicare vecchi messaggi relativi alla sessione K_{ab} che A considererebbe come provenienti da B. Il danno sarebbe massimo se M, per altre vie, fosse riuscito ad impadronirsi di K_{ab}.

Considerazioni simili possono essere fatte per B se questo processo riutilizza la quantità k_b.

ESERCIZIO 3

Quesito A. Il protocollo non garantisce l'identificazione. Supponiamo che un avversario A intercetti una coppia challenge-response. Più precisamente, A intercetta la challenge e la frame f che trasporta la relativa response. Tale frame oltre a response trasporta anche il vettore di inizializzazione v utilizzato per cifrare la challenge. Dalla challenge (testo in chiaro) e dalla response (crittogramma) è possibile ricavare il keystream $\{z_i(v)\}$ facendo l'or-esclusivo tra le due quantità. A questo punto l'avversario conosce una coppia (vettore di inizializzazione, keystream) $(v, \{z_i(v)\})$ che può riutilizzare in (un numero indefinito di) altre esecuzioni del protocollo di identificazione.

Quesito B. Come nel caso precedente l'avversario riesce a violare il protocollo riutilizzando una coppia $(v, \{z_i(v)\})$. Il keystream può essere ricavato come nel caso precedente mentre v può essere ricavato dalla frame che trasporta la challenge. Differentemente a prima, adesso è AP che seleziona v. L'avversario quindi deve costruirsi un dizionario $DIZ = \{(v, \{z_i(v)\}) \mid v \in V_{24}\}$, con V_{24} l'insieme di tutte le sequenze di 24 bit. DIZ ha 2^{24} voci, ciascuna di $sizeof(v) + sizeof(\{z_i(v)\})$ byte. La quantità v occupa 3 byte. Il keystream $\{z_i(v)\}$ ha per definizione la stessa dimensione della challenge, cioè 128/8 = 16 byte. Ne segue quindi che una voce del dizionario occupa 19 byte. Ne segue perciò che il DIZ ha una dimensione pari a $19 \times 2^{24} \cong 20$ Mbyte.