Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Appello del 24/04/2006

Non è ammesso alcun materiale per la consultazione (pena l'annullamento del compito). Avete due ore a disposizione. Buon lavoro!

1	2	3	4	totale
/20	/20	/30	/30	/100

1. (20 punti) Si descrivano gli algoritmi di cifratura, decifratura ed espansione della chiave nel crittosistema AES.

2. (20 punti) Siano h_1 ed h_2 due funzioni hash. Si mostri che se una tra le due funzioni soddisfa la proprietà di sicurezza debole, allora anche la funzione $h(x)=h_1(x)||h_2(x)$ soddisfa tale proprietà (il simbolo || denota la concatenazione di stringhe).

3. (30 punti) Crittosistema RSA.
    - (10 punti) Si descrivano le fasi di generazione delle chiavi, cifratura e decifratura. Inoltre, si mostri che le operazioni di cifratura e decifratura sono una l'inversa dell'altra.
    - (20 punti) Sia n=323 il modulo RSA di Alice.
        i. (10 punti) Si supponga che Oscar venga a conoscenza del valore $\Phi(n)=288$. Si illustri quali informazioni possono essere ricavate da Oscar, illustrando tutte le computazioni effettuate.
        ii. (10 punti) Sia e=35 l'esponente pubblico di Alice e sia C=23 un testo cifrato per Alice. Si mostri come Oscar sia in grado di risalire al testo in chiaro corrispondente, illustrando tutte le computazioni effettuate.

4. (30 punti) Message Authentication Code.

Alice vuole spedire un messaggio M ad *n* riceventi $B_1,\ldots, B_n$, assicurandone l'integrità e l'autenticità (non la confidenzialità). Alice decide di usare un MAC.

- (10 punti). Si supponga che Alice e $B_1,\ldots, B_n$, condividano una sola chiave k. Alice computa il MAC del messaggio M con chiave k e spedisce la coppia (messaggio, MAC) a ciascun B_i. Discutere la sicurezza di questa soluzione.
- (10 punti). Si supponga che Alice abbia a disposizione un insieme $X=\{k_1, \ldots, k_r\}$ di r chiavi (r<n) ed ogni utente B_i abbia un sottoinsieme $X_i \subseteq X$ di chiavi. Per ciascun utente B_i, Alice calcola il MAC del messaggio M con ciascuna delle chiavi contenute nell'insieme X_i e spedisce le varie coppie (messaggio, MAC) a B_i, che accetta M come valido solo se ha ricevuto tutti i MAC calcolati con le chiavi in X_i. Supponendo che i B_i non possano colludere, quale proprietà devono avere i sottoinsiemi X_i perché ciascun partecipante sia sicuro che il messaggio sia stato originato da Alice?
- (10 punti). Nella situazione descritta al precedente punto (b), si mostri che, nel caso n=6, ad Alice basta calcolare 4 MAC, fornendo un esempio di composizione dei sottoinsiemi $X_i \subseteq \{k_1, \ldots, k_4\}$, i=1,…, 6.