

**Crittografia esame del 13 dicembre 2006 minuti **

Nota: non tutte le domande hanno lo stesso valore!

Supponi che Bob usa un sistema RSA con una chiave difficile da fattorizzare. Alice invia un messaggio codificato a Bob in cui codifica ciascuna delle lettere del messaggio, lettera-per-lettera usando il sistema RSA usando ad esempio $A=10$, $B=11$, $C=12$, Descrivi come Trudy possa facilmente decodificare il messaggio senza rompere il sistema RSA. Suggestire una modifica del protocollo robusta che mantiene la codifica del messaggio lettera per lettera.

Uno schema MAC è considerato sicuro se un avversario non è in grado di creare una coppia valida Messaggio/MAC dopo aver visto anche molte coppie Messaggio/schema di sua scelta. Illustra uno schema per il calcolo del MAC di un messaggio di lunghezza qualsiasi che utilizza uno schema a blocchi tipo DES o AES. Discuti come la soluzione proposta resiste ad attacchi noti (compleanno, troncamento del messaggio ecc.).

Descrivi un metodo per l'autenticazione unidirezionale che autentica A rispetto a B ed utilizza timestamp e un solo messaggio. Spiega come mai per la sicurezza del protocollo è sufficiente che B memorizzi i timestamp ricevuti negli ultimi 10 minuti.

Con riferimento a SSL e TLS spiegare

- quale è lo scopo del codice "Change Cipher Spec" spiegando quando viene utilizzato e per quali motivi è stato introdotto.
- come il protocollo resiste ad attacchi di tipo replay nella fase di autenticazione (handshake).

IMS (Internet Music Station) distribuisce concerti dal vivo ai suoi membri in regola con il pagamento della quota associativa. I non membri o i membri che non hanno rinnovato la quota non devono poter ascoltare. IMS ha trovato uno schema che funziona con al più n clienti (sia attuali che utenti che abbiano disdetto). Per fare questo IMS distribuisce ai suoi utenti in regola un media player che utilizza $n+1$ chiavi $R_0, R_1, R_2, \dots, R_n$.

Si assumi per semplicità che $n = 10$. Siano $R_0, R_1, R_2, \dots, R_{10}$ numeri casuali di 512 bit. Il media player dato al cliente i contiene tutti numeri casuali tranne R_i (cioè contiene 10 chiavi). Sia S l'insieme dei sottoscrittori in regola. Il protocollo messo a punto da IMS funziona nel seguente modo: IMS all'inizio invia un messaggio in chiaro contenente S e quindi una chiave funzione dei sottoscrittori non in regola. Ad esempio se $S = \{1, 2\}$ allora la chiave calcolata è funzione di $R_0, R_3, R_4, \dots, R_{10}$. In questo modo gli utenti in S possono calcolare la chiave mentre gli utenti non in S non sono in grado di farlo.

a. Mostra come IMS possa costruire una chiave funzione tale che ogni utente in S possa calcolare K (usando le informazioni nel suo media player) mentre ogni utente fuori di S non sia in grado di calcolare K anche decrittando le informazioni nel suo mediaplayer (quando un utente non paga rimane comunque in possesso delle chiavi).

Giustifica brevemente come la tua soluzione sia in grado di soddisfare i requisiti.

b. Discuti se la tua soluzione resiste alle coalizioni; in particolare valuta se due utenti cancellati possono mettere insieme le informazioni a loro disposizione e costruire un nuovo media player.

NOTA: ci sono metodi molto migliori per questo problema!