

Crittografia e sicurezza delle reti esame del 20.12.2004
NB le domande non hanno lo stesso punteggio!

Spiegare l'importanza di generare numeri casuali nelle applicazioni crittografiche. Fornire le caratteristiche che un generatore di numeri casuali deve avere per essere utilizzabile in applicazioni crittografiche. Fornire un generatore di numeri casuali che utilizzi una funzione hash resistente alle collisioni.

Con riferimento a IPSEC spiegare

1. in quali scenari è utile la modalità tunnel e quali sono i vantaggi di questa modalità.
2. per quali motivi si possono avere più associazioni di sicurezza fra due entità (fornire esempi specifici)

Perché AES è considerato molto efficiente? come si realizza la moltiplicazione nel campo di Galois $GF(2^8)$? (max 4 righe)

Perché l'integrità del messaggio è importante nell'autenticazione? Rispondere fornendo almeno un esempio. (max 5 righe)

Esercizio: Supponi che Alice e Biagio condividano una chiave segreta K . Alice vuole mandare un messaggio a Biagio, a può usare solo MAC, cioè non può usare alcun metodo crittografico di codifica sicura.

1. Mostra come Alice può codificare un messaggio m usando solo funzioni MAC. (sugg. codifica il messaggio bit a bit)
2. Mostra come Alice può anche garantire autenticità, cioè nessun attaccante attivo è in grado di modificare il messaggio stesso.

*SOLUZ.: 1 non va bene uso di MAC di codifica di ciascun bit con lo stesso padding perché si possono avere attacchi di sostituzione. Due possibilità: a) codifica MAC di un messaggio bit a bit con PADDING VARIABILE per ogni bit (es. MAC(il primo bit del messaggio è 0) poi MAC(il secondo bit del messaggio è ...) b) uso di un meccanismo tipo CBC: codifico messaggio bit a bit con padding anche uguale (la variabilità della codifica è data dal meccanismo CBC)
2. faciel faccio MAC di tutto quanto è stato spedito*

Esercizio: Una società fornisce una soluzione per aiutare i clienti a riconoscere siti di commercio elettronico. Lo scopo è evitare che gli utenti forniscano le loro password a siti falsi (che appaiono identici ai siti a cui l'utente si vuole connettere. Quando un cliente usa questa soluzione fornisce una username e aspetta un'immagine che lui ha scelto precedentemente; quando vede l'immagine scelta il cliente sa che è collegato con il sito vero e non uno falso. In questo modo l'utente è sicuro di essere collegato al sito vero e non a uno falso. fornire la sua password. Si assume ovviamente che la scelta dell'immagine sia fatta la prima volta con il sito autentico. L'immagine scelta viene fornita ogni volta che si collega.

Si assuma una soluzione di questo tipo. Si supponga che l'avversario possa intercettare e fare spoofing di messaggi.

La società può scegliere di memorizzare l'immagine nel server o nel computer del cliente.

1. Fornire un attacco di uomo nel mezzo nel caso che l'immagine sia memorizzata nel server. L'attacco deve permettere ad un falso sito di fornire l'immagine scelta dall'utente.
2. Una tecnica per evitare l'attacco è l'utilizzo dei cookie – le informazioni che l'utente fornisce quando si collega. Spiegare come si possa utilizzare queste informazioni (sugg. il cookie – che è un numero intero – deve cambiare di volta in volta).

Soluz.: 1. attacco uomo nel mezzo: l'attaccante si fa dare l'immagine dal server e poi la propone al client.

2. serve un meccanismo di autenticazione dell'utente. l'utilizzo di chiave pubblica non è ragionevole dato il contesto (quanto di voi hanno una chiave pubblica certificata?). Una soluzione semplice è quella di mettersi d'accordo la prima volta per il valore del cookie e poi cambiarlo di volta in volta usando un generatore di numeri pseudocasuali; ovviamente il generatore è lo stesso usato da client e server. (in questo modo la conoscenza di una sequenza di cookie non permette all'avversario di ottenere il numero successivo e quindi di generare il prossimo cookie per ottenere l'immagine dal server.