Soluzione dello scritto del 26 giugno 2023

Crittografia

1. Dare la definizione di PRG (PseudoRandomGenerator) e, quindi, di cifrari a flusso (*stream cipher*). Un cifrario a flusso può essere perfettamente sicuro? Dare la definizione formale di PRG impredicibile e connetterla con la definizione di PRG sicuro.

Le risposte sono nel pacco di lucidi `crittografia/02-stream-ciphrs.pdf`.

2. Descrivere il protocollo di Diffie-Hellman (idea ad alto livello, descrizione protocollo e analisi sicurezza/attacchi).

Le risposte sono nel pacco di lucidi `crittografia/05-key-exchange.pdf`.

Sicurezza

1. Descrivere un esempio pratico di *security by obscurity* e un attacco al sistema in esame.

Un possibile esempio è l'occultamento del SSID: si nasconde la rete senza fili agli occhi dell'attaccante, facendo sì che debba scoprirne il nome per poter tentare un collegamento.

Un possibile attacco è origliare i pacchetti di richiesta di connessione da parte dei nodi che legittimamente chiedono l'accesso. Essi inviano il SSID in chiaro.

2. Descrivere il meccanismo di *challenge* e *response* e come potrebbe essere usato per migliorare la sicurezza dell'apertura delle automobili. Descrivere inoltre almeno un attacco a un sistema che utilizza *challenge* e *reponse*.

La descrizione è presente nel pacco di lucidi `generale/03-radio-e-wireless.pdf`.

Quando il telecomando invia un comando all'automobile, questa potrebbe inviargli un *nonce*. Solo se il *nonce* è restituito correttamente crittografato il comando originale viene eseguito.

Siccome il *nonce* è invitato in chiaro, tutti i *Known Plaintex Attacks* sono potenziali attacchi a questo sistema.

Laboratorio

1. È sensato eseguire un attacco con le Rainbow Tables in caso di *hash* di password con *salt*?

Nel caso generale no, poiché esse sono un attacco precomputato e sono quindi rese inutilizzabili dal sale, che viene estratto casualmente.

Fa eccezione il caso in cui, per qualche motivo, si sia già a conoscenza del sale prima dell'attacco e si abbia il tempo di generare una tabella arcobaleno ad-hoc per tale sale.