Esercizi Capitoli 7 ed 8

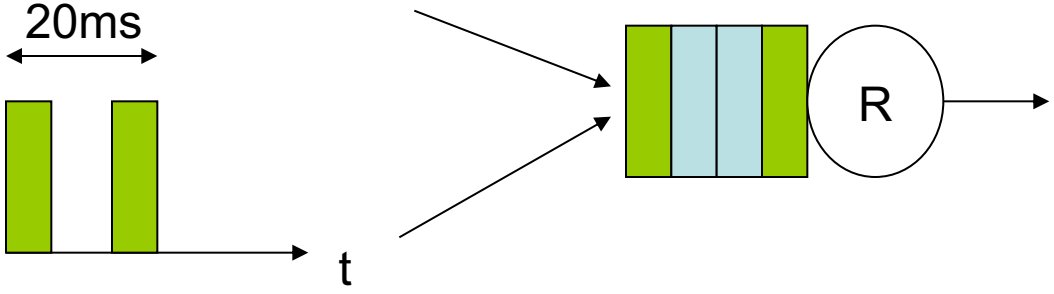
5 min. per pensare 5 min. per discutere la soluzione

Jitter

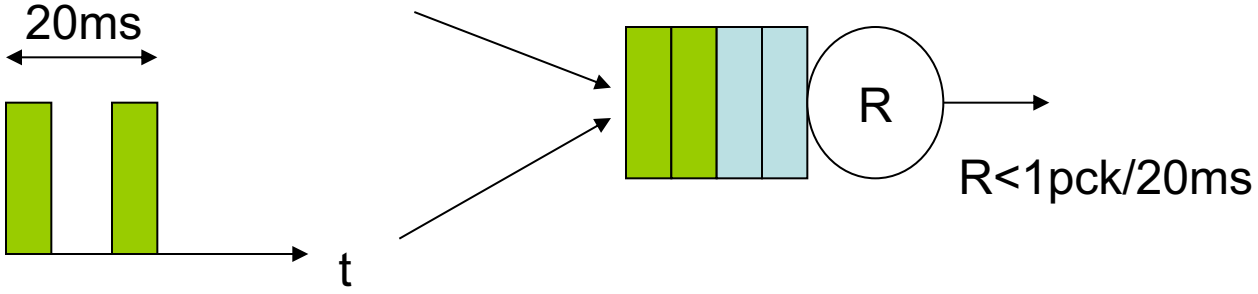
- Supponiamo che un trasmittente invii pacchetti ogni 20ms
- Perchè posso ottenere pacchetti in ricezione i cui istanti di ricezione siano >20ms
- Perchè posso ottenere pacchetti in ricezione i cui istanti di ricezione siano <20ms
- Come faccio ad ottenere una riproduzione sincrona anche in presenza di jitter?
- Qual’è il legame tra ritardo di riproduzione e la perdita di pacchetti?

Jitter

- Perchè posso ottenere pacchetti in ricezione i cui istanti di ricezione siano >20ms

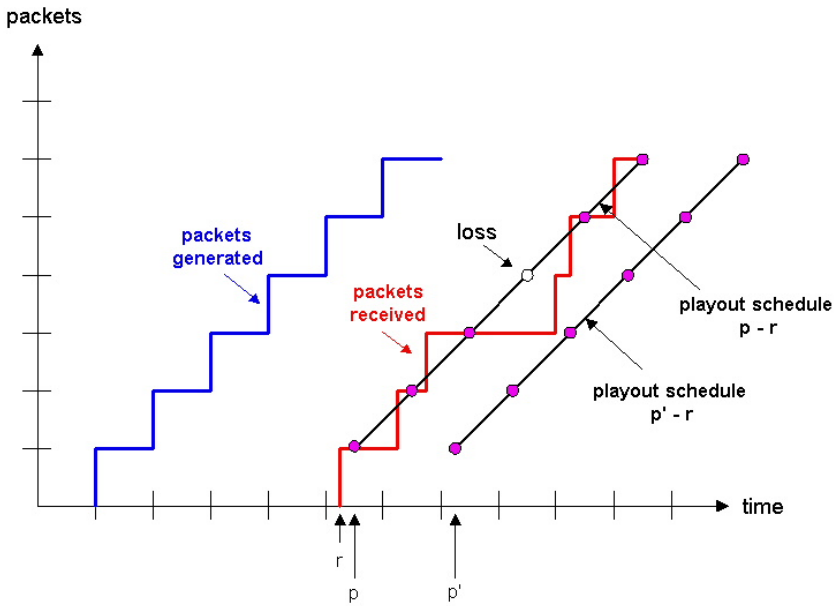


- Perchè posso ottenere pacchetti in ricezione i cui istanti di ricezione siano <20ms



Jitter

- Come faccio ad ottenere una riproduzione sincrona anche in presenza di jitter?
  - Numero di sequenza
  - Marcatura temporale
  - Ritardo riproduzione
- Qual'è il legame tra ritardo di riproduzione e la perdita di pacchetti?



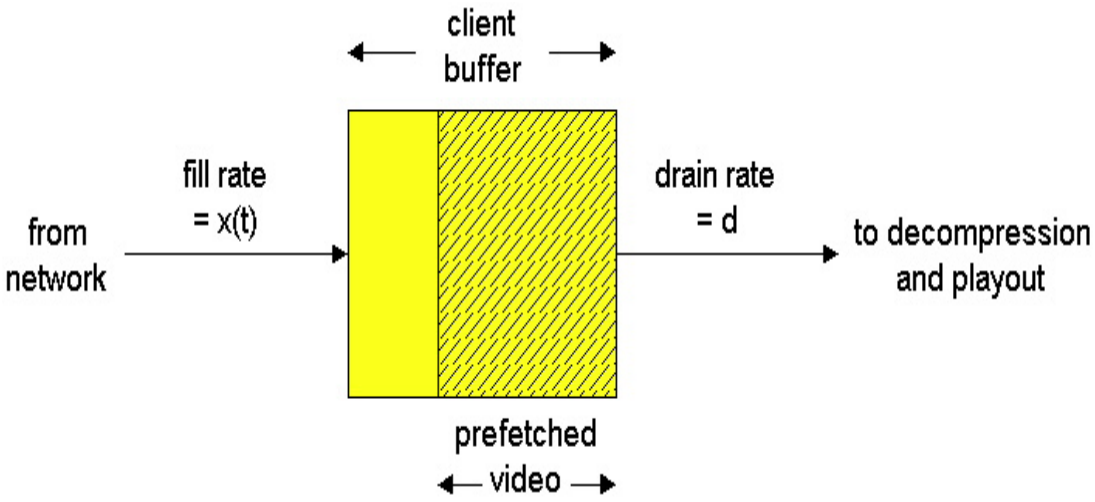
Ritardo di riproduzione adattativo

- Per quale motivo è utile
- Come stimo il ritardo di riproduzione d_i?
- Come stimo l'istante di riproduzione p_i?
- Supponendo che un pacchetto sia inviato ogni 20ms come determino il primo pacchetto di un periodo di riproduzione
- In caso di perdite?

Ritardo di riproduzione adattativo

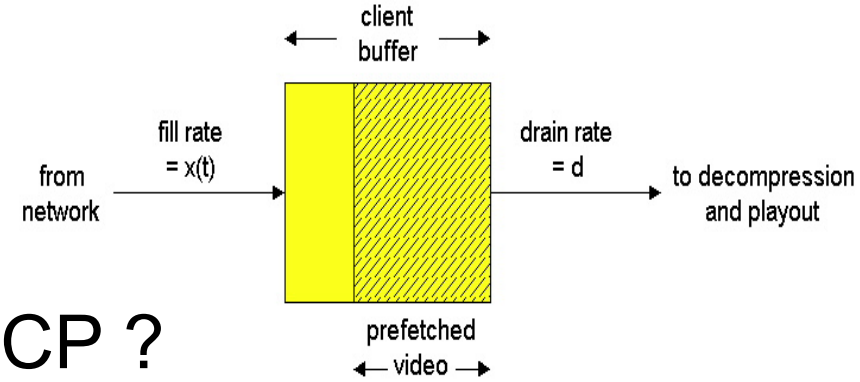
- Intervalli silenzio/parlato
- Come stimo il ritardo d_i?
  - $d_i = (1-u)\, d_{i-1} + u\,(r_i - t_i)$
- Come stimo l'istante di riproduzione p_i?
  - $p_i = t_i + d_i + K\, v_i$
- Supponendo che un pacchetto sia inviato ogni 20ms come determino il primo pacchetto di un periodo di riproduzione
  - $t_i - t_{i-1} > 20ms$
- In caso di perdite?
  - numeri di sequenza

Buffer del client in reti multimediali



- Cosa succede se uso TCP ?
- Cosa succede se usiamo TCP, la larghezza di banda TCP è molto maggiore di d e il buffer può contenere solo 1/3 delle dimensioni del file ?

Buffer del client in reti multimediali



- Cosa succede se uso TCP ?
  - x(t) fluttua nel tempo a causa di controllo di congestione
  - Perdita pacchetti → x(t) può essere inferiore a d per molto tempo → svuotamento del buffer
- Cosa succede se usiamo TCP, la larghezza di banda TCP è molto maggiore di d e il buffer può contenere solo 1/3 delle dimensioni del file ?
  - Quando il buffer è pieno (o semi-pieno) blocco o rallento x(t) → fluttuazione di x(t) intorno a d → aumento probabilità di starvation

Codici a Correzione di Errore

1. Si consideri un codice a correzione di errore per un segnale vocale con codifica PCM che introduca un pacchetto di recupero ogni due pacchetti dati.
2. Si consideri inoltre una codifica interleaving che opera su insiemi di tre blocchi formati ognuno da tra pacchetti, due dati ed il corrispondente pacchetto di recupero.

Codici a Correzione di Errore

- Si determini la massima lunghezza di un singolo burst di perdita di pacchetti a cui la codifica è tollerante
- Si determini il minimo ritardo di riproduzione introdotto dalla codifica
- Si determini lo spreco di banda introdotto.

Buffer TCP e applicazione

- Che differenza c'è tra il buffer TCP e il buffer dell'applicazione?
  - Il client legge dati dal buffer TCP e li mette nel buffer dell'applicazione
  - Se il buffer dell'applicazione è pieno smetto di leggere pacchetti da buffer TCP finchè non si crea spazio

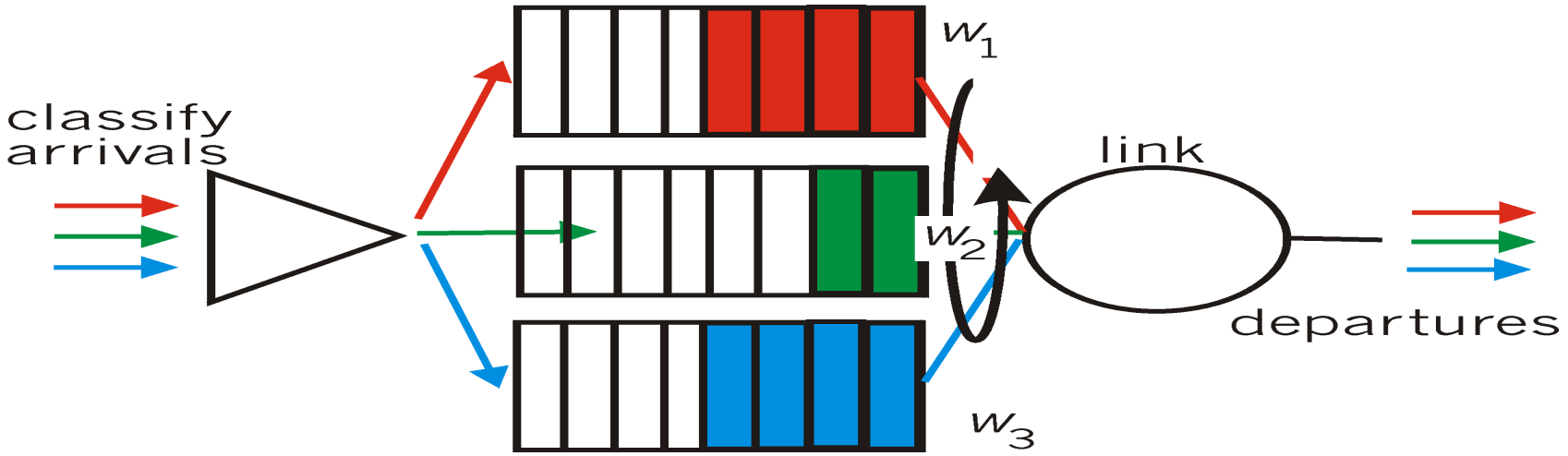
RTP

- Consideriamo una sessione RTP con 4 utenti che inviano e ricevono pacchetti RTP allo stesso indirizzo multicast. Ogni utente spedisce video a 100Kbps
  - A quale ritmo RTCP limiterà il suo traffico?
  - Quanta banda RTCP sarà allocata al ricevente e quanta al trasmittente?

RTP/RTCP

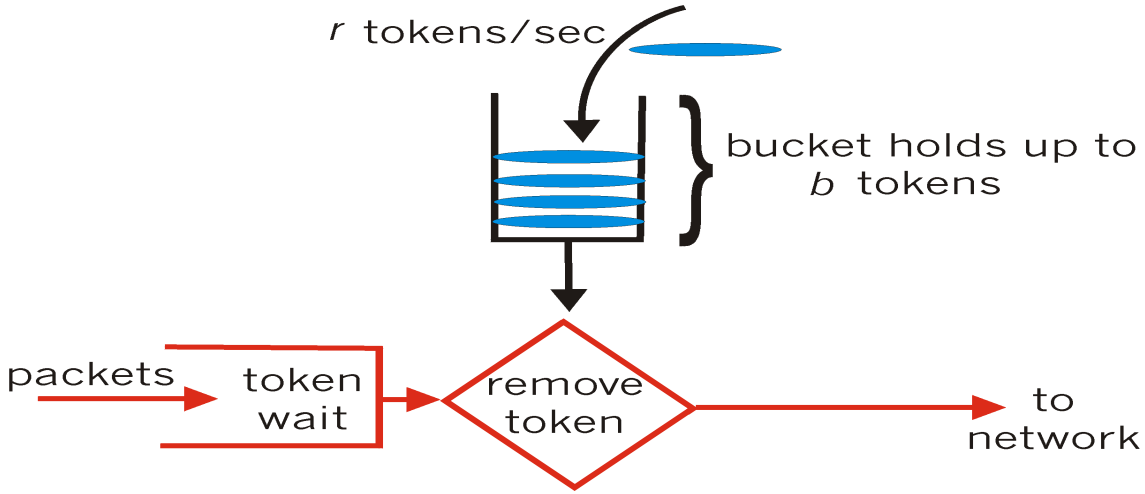
- Consideriamo una sessione RTP con 4 utenti che inviano e ricevono pacchetti RTP allo stesso indirizzo multicast. Ogni utente spedisce video a 100Kbps
  - A quale ritmo RTCP limiterà il suo traffico?
    - $T_{sender} = \frac{\text{\# senders * avg RTCP pkt size}}{\text{.25 * .05 * RTP bandwidth}}$
    - $T_{rcvr} = \frac{\text{\# receivers * avg RTCP pkt size}}{\text{.75 * .05 * RTP bandwidth}}$
  - Quanta banda RTCP sarà allocata al ricevente e quanta al trasmittente?
    - la banda totale usata è 4*100Kbps=400Kbps → 5% per RTCP = 20Kbps
    - Poichè ciascun utente è sia ricevente che trasmittente → 20/4=5Kbps (in generale 25% tx, 75% rx)

WFQ

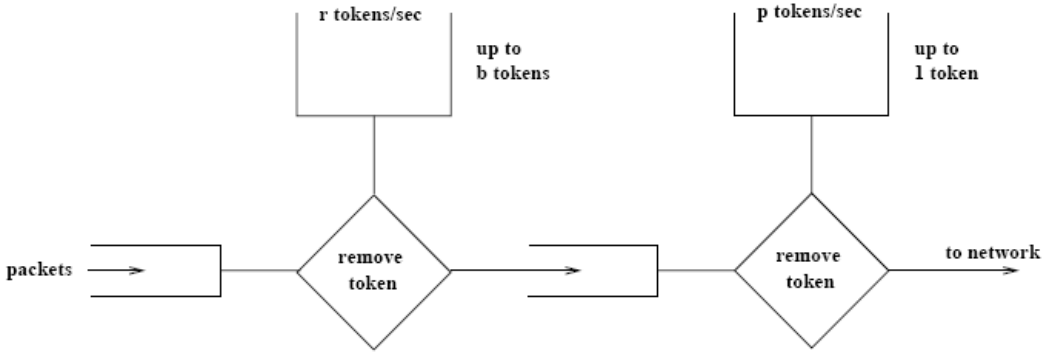


- w1=0.5, w2=0.25, w3=0.25
- Supponiamo ci sia un gran numero di pacchetti nel buffer:
  - Se round robin 123123123123123, WFQ?
  - 1213121312131213….

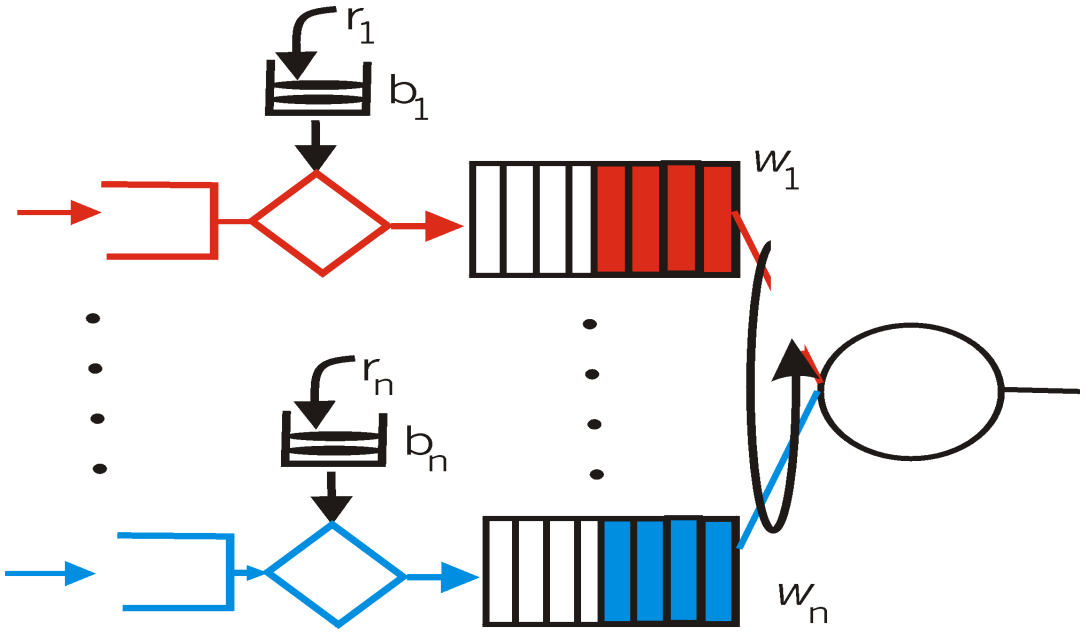
Leaky Bucket



- Tasso medio?
- Burst?
- Picco?

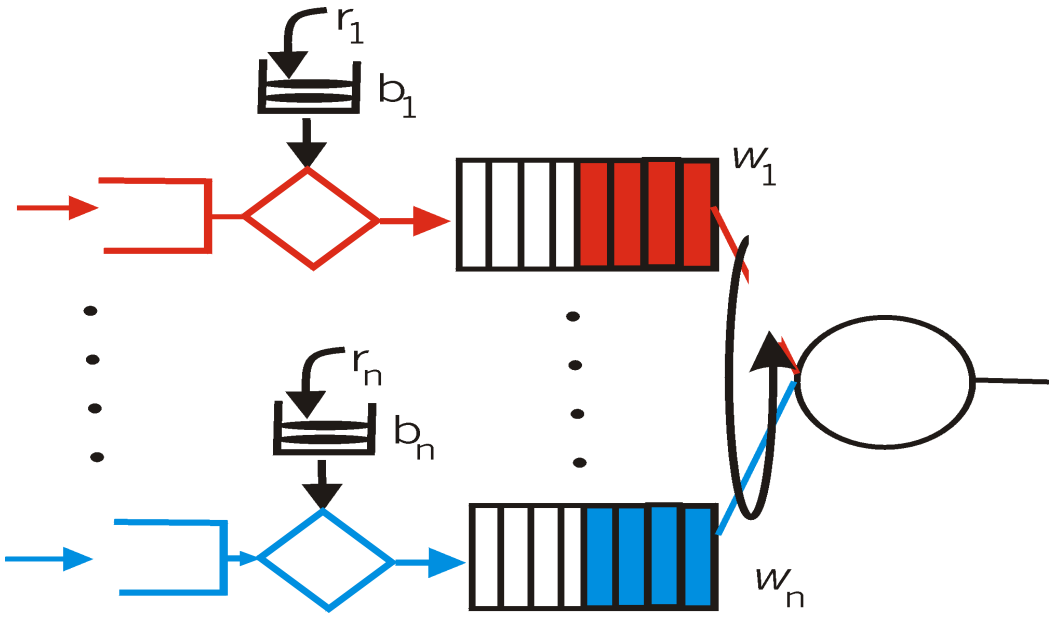


Ritardo massimo



- Qual'è il ritardo massimo se il secchio è pieno e arriva un burst di b1 pacchetti sulla coda 1?
- E il ritardo di pacchetti non appartenenti al burst?

Ritardo massimo



- I pacchetti vengono serviti ad un tasso pari almeno a $R\ w_i / \sum_j w_j$
- L'ultimo pacchetto del burst accumula un rutardo pari a $b_i / (R\ w_i / \sum_j w_j)$
- $r_1 < \frac{W_1}{\sum W_j} R$ → $b_i / (R\ w_i / \sum_j w_j)$

Esercizi

1. Descrivere graficamente un protocollo di autenticazione basato su chiave pubblica che risulta vulnerabile rispetto ad un attacco del tipo "uomo nel mezzo".

   Il protocollo è più sicuro se l'autenticazione è richiesta da entrambi le parti?

   Discutere brevemente inoltre le modalita' con cui è possibile rendere robusto il protocollo rispetto a questo tipo di attacchi.

Autenticazione: X.509

- Y{I} rappresenta la firma di I da parte di Y
- t timestamp, r nonce (num. casuale)
- A ⟶ B: $A\{t_A, r_A, B\}$
- B ⟶ A: $B\{t_B, r_B, A, r_A\}$

- Se Trudy usa messaggi di autentica usati precedentemente (replay di messaggi) per sostituirsi a A allora il time stamp è cambiato
- Firma di r_B da parte di A fornisce ulteriore prova a B sulla sua identità

Autenticazione: X.509 (cont.)

- Autenticazione tridirezionale

- A ⟶ B: $A\{t_A, r_A, B\}$
- B ⟶ A: $B\{t_B, r_B, A, r_A\}$
- A ⟶ B: $A\{r_B\}$

- Il terzo messaggio rappresenta ulteriore prova per B che sta parlando con A

Autenticazione: X.509 (cont.)

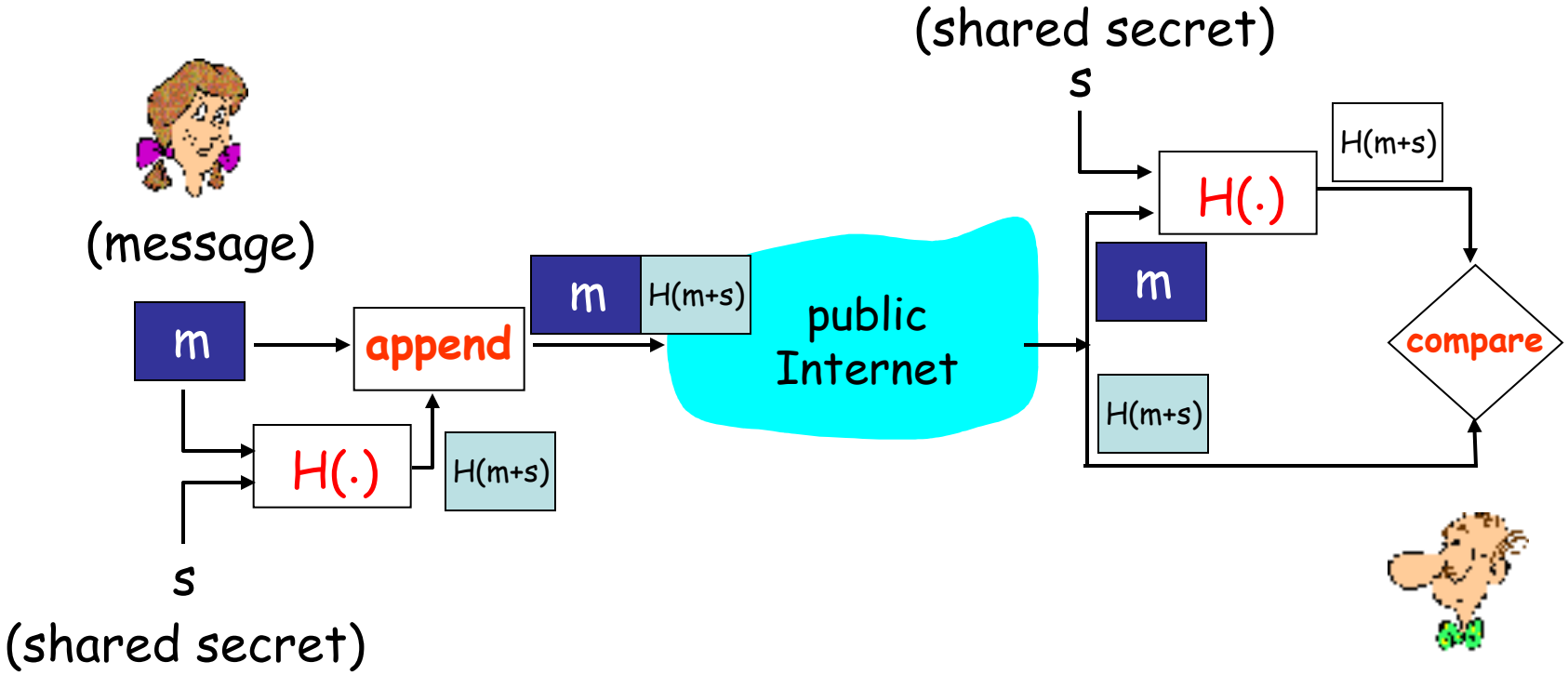
- Autenticazione tridirezionale con timestamp facoltativo (versione vecchia di X.509)
- A ⟶ B: $A\{r_A, B\}$
- B ⟶ A: $B\{r_B, A, r_A\}$
- A ⟶ B: $A\{r_B\}$

- La sicurezza si basa sul fatto che i nonce non sono utilizzati più volte
- Sufficiente?

Esercizi

- 2. Descrivere graficamente un metodo per il calcolo dell'impronta di un documento che utilizza DES (e calcola impronte di 64 bit). Infine spiegare in dettaglio perche' impronte di 64 bit non sono considerate sicure (indipendentemente dal metodo utilizzato per il calcolo).

Message Authentication Code



Esercizi

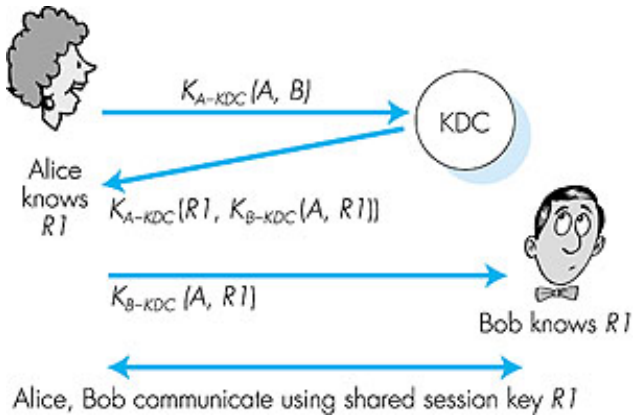
- 3. Assumete che un KDC server o un CA server si guasti. Chi può comunicare in modo sicuro e chi no nei due casi?

KDC

- 1.1 Qual'è il vantaggio di usare una Key Distribution Center (KDC) rispetto ad avere una chiave per ogni coppia di utenti? Quantificare la risposta nel caso di N utenti.
- 1.2 Qual informazione deve essere condivisa tra il KDC e ciscun utente?
- 1.3 Come si fa a condividere una chiave di sessione usando un KDC?
- 1.4 Che differenza c'è tra una Key Distribution Center (KDC) ed una Certification Authority (CA)?

Autorità di certificazione (Key Distribution Center (KDC))

- Alice e Bob vogliono condividere una chiave segreta R (di sessione)
- KDC condivide chiavi segrete con ogni utente ($K_{A\text{-}KDC}$ [$K_{B\text{-}KDC}$] con A [B])



- Alice comunica con KDC, prende la chiave di sessione R e $K_{B\text{-}KDC}(A,R)$ (chiave, utile per comunicare con A, codificata con $K_{B\text{-}KDC}$)
- Alice comunica a Bob $K_{B\text{-}KDC}(A,R1)$
- Bob estrae R da $K_{B\text{-}KDC}(A,R)$

Alice e Bob condividono la chiave segreta R

Digest

- Illustrare e motivare un esempio in cui è utile calcolare il digest (l'impronta) di un messaggio.
- Spiegare per quale motivo l'utilizzo del check sum (controllo di parità) usato dal protocollo IP non è una buona scelta per il calcolo del digest di un pacchetto.

Chiave Simmetrica vs Chiave Simmetrica

- Fornire una spiegazione intuitiva dei motivi che sono alla base della sicurezza della crittografia a chiave asimmetrica e motivare anche intuitivamente per quale motivo la crittografia a chiave asimmetrica è estremamente più lenta di quella a chiave simmetrica.

CHECKSUM

- Messaggio

I O U 1 → 9

0 0 . 9 → 1

9 B O B

900.19
"IOU900.19BOB"

100.99
"IOU100.99BOB"

- ASCII

49 4F 55 31 → 39

30 30 2E 39 → 31

~~39 42 4F 42~~

B2 C1 D2 AC
(checksum)

I due messaggi hanno
la medesima checksum,
ma un costo decisamente superiore!

Digest

- In cosa consiste il paradosso del compleanno?
- Che relazione c'è tra tale paradosso e la sicurezza di un algoritmo che calcola l'impronta digitale?
- Supponiamo di disporre di risorse computazionali sufficienti per generare in un minuto 264 combinazioni di numeri.
- Quale è il numero di bit minimo per l’impronta digitale affinchè sia necessario un secolo per generare due documenti con uguale impronta?

Un possibile attacco (cont.)

- Paradosso del compleanno

❒ Quante persone bisogna scegliere a caso affinchè con prob.>0.5 ci sia una persona con lo stesso mio compleanno? Risposta 183

❒ Quante persone bisogna scegliere a caso affinchè con prob.>0.5 ci siano almeno due persone con lo stesso compleanno? Risposta solo 23.

Prob(scelgo t elementi diversi fra n)=

(1- (t-1)/n) (1- (t-2)/n)…. (1- 2/n) (1- 1/n)=

~ $e^{(-t(t-1)/2n)}$

con t =23 e n=365 si ottiene prob. > 0.5

t

2

1

Ecommerce

- Un compratore si rivolge ad un sito di commercio elettronico.
- Quali strumenti garantiscono il compratore dell'identitità del sito di commercio elettronico e viceversa.

Chiave Segrta di Sessione

- Si illustrino vaie modalita' di concordare su una chiave segreta di sessione nel caso di
- i) un sito di commercio elettronico;
- ii) all'interno di una rete locale;
- iii) tra due router IPSEC.

- Due utenti A e B conoscono con certezza la chiave pubblica dell'altro; sia KSA la chiave segreta di A.
- Il seguente protocollo di autenticazione di A non e' sicuro
-
- A --> B: sono A
- A --> B: N (nonce scelto a caso da A)
- A --> B: KSA (N) (Codifica di N con la chiave segreta KAB)